Guide de l'utilisateur du logiciel Cisco Secure Workload sur site, version 3.8

Première publication : 2023-05-19

Dernière modification : 2023-10-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

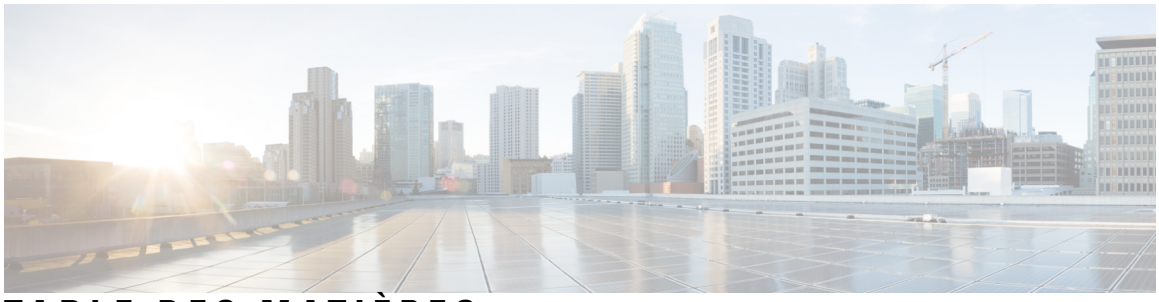
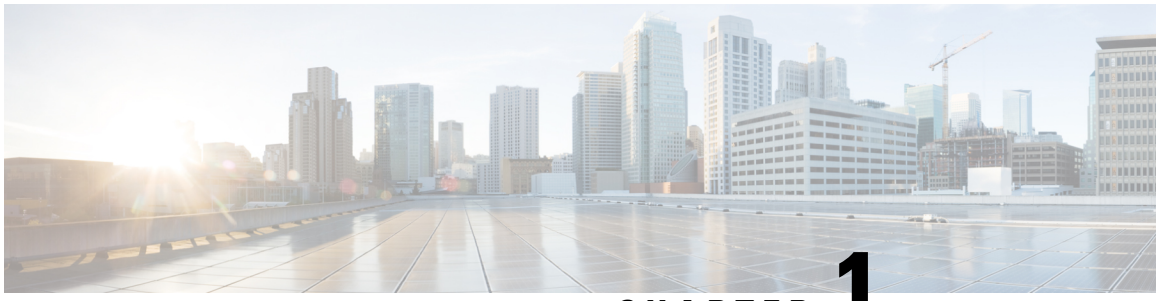


TABLE DES MATIÈRES



CHAPTER 1

Get Started

Navigateurs pris en charge

Cisco Secure Workload prend en charge les navigateurs Web suivants :

- Google Chrome
- Microsoft Edge

Assistant de démarrage rapide

Un assistant facultatif peut vous guider dans la création de la première branche de votre arborescence de portée, qui est une première étape vers la génération et l'application de politiques à l'application de votre choix. L'assistant présente les concepts et les avantages des étiquettes et de la portée.

Les rôles d'utilisateur suivants peuvent accéder à l'assistant :

- Administrateur de site
- Assistance technique
- Propriétaire de portée racine

Pour accéder à l'assistant, effectuez l'une des opérations suivantes :

- Connectez-vous à Cisco Secure Workload.
- Cliquez sur le lien dans la bannière bleue. La bannière bleue s'affiche en haut de toutes les pages.
- Cliquez sur **Overview** (Présentation) dans le menu principal.

Remarque Vous ne pouvez pas accéder à l'assistant si des portées sont déjà définies dans **Organize(Organiser)** > **Scopes and Inventory(Portées et inventaire)** . Supprimez les portées existantes pour accéder à l'assistant.

Premiers pas avec la segmentation et la microsegmentation

Utilisez les procédures générales données ici pour configurer des politiques de segmentation et de microsegmentation à l'aide de Cisco Secure Workload.

Processus général de mise en œuvre de la microsegmentation

Le but de la segmentation et de la microsegmentation est de n'autoriser que le trafic nécessaire à des fins commerciales et de bloquer tout autre trafic.

Procédure

Étape 1 Vérifiez que Cisco Secure Workload prend en charge les plateformes et les versions sur lesquelles vos charges de travail s'exécutent, et les systèmes qui fournissent des informations essentielles à vos politiques. Reportez-vous à la section Matrice de compatibilité de Cisco Secure Workload.

Étape 2 Installer les agents sur les charges de travail.

Les agents recueillent les données de flux et d'autres informations nécessaires à Cisco Secure Workload pour regrouper les charges de travail et déterminer les politiques appropriées. Les agents appliquent également les politiques approuvées. Pour en savoir plus, y compris les liens vers les listes des plateformes prises en charge et la configuration requise, consultez Déployer des agents logiciels.

Étape 3 Rassemblez ou téléversez des étiquettes qui décrivent vos charges de travail.

Les étiquettes vous permettent de comprendre facilement l'objectif de chaque charge de travail et fournissent d'autres renseignements clés sur chaque charge de travail.

Vous avez besoin de ces informations pour regrouper les charges de travail, appliquer les politiques appropriées et comprendre les politiques suggérées par Cisco Secure Workload. Les étiquettes constituent la base de la gestion des groupes qui simplifient la gestion des politiques. Pour en savoir plus, consultez les sections Étiquettes de charge de travail et Importation d'étiquettes personnalisées, à la page 356.

Étape 4 Créez une arborescence de portée en fonction de vos étiquettes de charge de travail.

Les groupes logiques de charges de travail que les étiquettes vous aident à créer sont appelés portées, et un ensemble d'étiquettes bien choisi vous aide à créer une carte hiérarchique de votre réseau appelée arborescence de portées. Cette vue hiérarchique des charges de travail sur votre réseau est essentielle pour créer et maintenir efficacement des politiques. La vue hiérarchique vous permet de créer une politique une seule fois et de l'appliquer automatiquement à chaque charge de travail sur cette branche de l'arborescence. Cette vue vous permet également de déléguer la responsabilité de certaines applications (ou parties de votre réseau) à des personnes qui ont l'expertise nécessaire pour déterminer les politiques appropriées pour ces charges de travail.

Vous pouvez interroger les charges de travail et les regrouper dans des portées en fonction de leurs étiquettes. Par exemple, vous pouvez créer un portée appelée App Courriel qui inclut toutes les charges de travail ayant les étiquettes Application = App Courriel et Environnement = Production. Vous pouvez créer une portée parente pour la portée Application = App Courriel en utilisant la requête Environnement = Production. La portée de la production comprend l'application de courriel de production et toutes les autres charges de travail étiquetées Environnement = Production.

Pour en savoir plus, consultez Portées et inventaire.

Si vous n'avez encore créé aucune portée, vous pouvez utiliser l'assistant de démarrage rapide pour créer une arborescence de portées. Pour en savoir plus, consultez Assistant de démarrage rapide, à la page 1.

Étape 5 Créez un espace de travail pour chaque portée pour laquelle vous souhaitez créer des politiques.

L'espace de travail est l'endroit où vous gérez les politiques pour les charges de travail de cette portée. Pour en savoir plus, consultez Utiliser des espaces de travail pour gérer les politiques.

Étape 6 Créez manuellement des politiques qui s'appliquent à votre réseau.

Par exemple, vous pouvez autoriser l'accès de toutes les charges de travail internes à votre serveur NTP et refuser tout le trafic externe, ou refuser l'accès de tous les hôtes non internes, à moins que cela ne soit explicitement autorisé. Les politiques peuvent être absolues, ce qui signifie qu'elles ne peuvent pas être remplacées par des politiques plus spécifiques, ou par défaut, où elles peuvent être remplacées par des politiques plus spécifiques.

Pour en savoir plus, consultez Créer manuellement des politiques, à la page 441.

Cisco Secure Workload propose des modèles de politiques qui facilitent la création de ces dernières. Pour en savoir plus, consultez Modèles de politiques, à la page 445.

Vous pouvez appliquer les politiques créées manuellement sans attendre qu'elles soient découvertes. Pour en savoir plus, consultez Appliquer des politiques, à la page 558.

Étape 7 Détectez automatiquement les politiques en fonction des schémas de trafic existants.

Cisco Secure Workload analyse le trafic entre les charges de travail, regroupe les charges de travail en fonction de leur comportement et propose un ensemble de politiques visant à autoriser le trafic dont votre entreprise a besoin pour que vous puissiez bloquer tout autre trafic.

L'analyse d'un plus grand nombre de flux de données sur une période plus longue permet de formuler des suggestions de politiques plus précises.

Vous pouvez découvrir les politiques de manière itérative. Vous trouverez plus d'informations à ce sujet dans la suite de cette procédure).

1. Découvrez les politiques pour une branche de votre arborescence de portée.

   Si vous venez de commencer, vous pouvez avoir un ensemble temporaire de politiques en place et fournir une protection contre les menaces futures.

2. Découvrez les politiques des portées uniques.

   En règle générale, vous effectuez cette opération pour les portées qui se trouvent au bas de votre arborescence ou près du bas de celle-ci. Ces portées comprennent généralement les charges de travail pour une seule application.

Pour en savoir plus, consultez Découvrir automatiquement les politiques et Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453.

Étape 8 Examinez et analysez vos politiques.

Examinez attentivement vos politiques pour vous assurer qu'elles produisent les effets escomptés et qu'il n'y a pas d'effets secondaires imprévus.

Collaborez avec des experts de domaine et des propriétaires d'applications de votre organisation pour comprendre les besoins et la pertinence des politiques suggérées.

a) Passez en revue les politiques et les grappes suggérées par Cisco Secure Workload.

(Les grappes sont des groupes de charges de travail au sein d'un portée qui sont étroitement liées et peuvent nécessiter des politiques plus adaptées que les politiques visant l'ensemble de la portée. Pour en savoir plus, consultez Regroupement des charges de travail : grappes et filtres d'inventaire, à la page 504).

Pour en savoir plus, consultez Consulter les politiques découvertes automatiquement, à la page 538.

b) Analysez vos politiques pour voir leur incidence sur le trafic réel sur votre réseau.

Utilisez l'analyse des politiques et les autres outils de Cisco Secure Workload pour confirmer que vos politiques autorisent le trafic dont votre entreprise a besoin pour exercer ses activités. Pour en savoir plus, consultez Analyse des politiques en temps réel et Représentation visuelle des politiques, à la page 542.

Lorsque vous analysez les résultats de vos politiques, gardez les points suivants à l'esprit :

- Les politiques dans les espaces de travail pour les portées supérieures d'une branche peuvent affecter les charges de travail des portées inférieures de la branche. Pour en savoir plus, consultez Héritage des politiques et arborescence de portée, à la page 438.
- La microsegmentation crée un pare-feu miniature autour de chaque charge de travail. Pour qu'une connexion soit réussie, le consommateur et le fournisseur de la transaction doivent avoir des politiques autorisant le trafic. Si les deux charges de travail ne se trouvent pas dans la même portée, la création de ces politiques peut nécessiter des étapes supplémentaires. Pour en savoir plus, consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 522.

Étape 9 Détectez les politiques de façon itérative, en fonction des besoins.

Un flux de trafic plus important produit des suggestions de politiques plus précises. Par exemple, pour un rapport mensuel, même trois semaines de données peuvent ne pas saisir tout le trafic essentiel. Continuez de découvrir les politiques et passer en revue et analyser de nouvelles suggestions de politiques. Chaque exécution de découverte propose des politiques en fonction des flux de trafic actuels.

Vous pouvez également procéder à une découverte itérative des politiques afin de prendre en compte les modifications apportées aux paramètres de découverte des politiques et aux grappes approuvées. Pour en savoir plus, consultez Réviser les politiques de manière itérative, à la page 481.

Avant de réexécuter la découverte automatique des politiques, assurez-vous d'approuver les politiques et les grappes que vous souhaitez conserver.

Chaque fois que vous redécouvrez des politiques, vous devez les passer en revue et les analyser.

Étape 10 Lorsque vous êtes prêt, appliquez les politiques.

Une fois que vous avez déterminé que les politiques associées à un espace de travail (et donc la portée associée) sont appropriées et qu'elles bloqueront le trafic indésirable sans interrompre les services essentiels, vous pouvez appliquer ces politiques.

Vous pouvez appliquer les politiques de manière itérative; par exemple, vous pourriez initialement appliquer uniquement les politiques créées manuellement dans des portées situés près du sommet de votre arborescence, puis, au fil du temps, appliquer les politiques découvertes dans des portées inférieurs de l'arborescence.

Pour en savoir plus, consultez Appliquer des politiques, à la page 558.

Configurer la microsegmentation pour les charges de travail s'exécutant sur des machines sans système d'exploitation ou des machines virtuelles

Procédure

Étape 1 Rassemblez les adresses IP des charges de travail sur votre réseau.

Pour chaque charge de travail, vous voudrez également le nom de l'application, le propriétaire de l'application, l'environnement (de production ou hors production) et d'autres renseignements comme la région géographique qui détermineront les politiques à appliquer.

Si vous n'avez pas de base de données de gestion des configurations (CMDB), vous pouvez recueillir cette information dans une feuille de calcul.

Pour commencer, choisissez une seule application sur laquelle vous pouvez vous concentrer.

Étape 2 Installez les agents sur les charges de travail virtuelles ou sans système d'exploitation prises en charge.

Pour en savoir plus, consultez la section Déployer des agents logiciels.

Étape 3 Téléchargez des étiquettes qui décrivent ces charges de travail.

Pour en savoir plus, consultez les sections Étiquettes de charge de travail et Importation d'étiquettes personnalisées, à la page 356.

Vous pouvez également exécuter l'assistant de démarrage rapide pour créer des étiquettes et la première branche de votre arborescence de portée . Pour en savoir plus sur l'assistant, consultez Assistant de démarrage rapide.

Étape 4 Si nécessaire, créez ou mettez à jour votre arborescence de portée en fonction de vos étiquettes.

Pour en savoir plus, consultez Portées et inventaire.

Étape 5 Créez un espace de travail pour chaque portée pour laquelle vous souhaitez appliquer des politiques.

Pour en savoir plus, consultez Utiliser des espaces de travail pour gérer les politiques.

Étape 6 Créez des politiques manuelles qui s'appliquent à votre réseau.

Pour en savoir plus, consultez Créer manuellement des politiques, à la page 441.

Étape 7 Pour en savoir plus sur les politiques spécifiques à la plateforme, consultez Politiques spécifiques à la plateforme, à la page 488.

Étape 8 Détectez automatiquement les politiques dans les espaces de travail associés à des portées de niveau inférieur.

Pour en savoir plus, consultez Découvrir automatiquement les politiques et ses sous-sections.

Étape 9 Examinez et analysez les politiques suggérées.

Pour en savoir plus, consultez Examiner et analyser les politiques, à la page 538 et les sous-sections.

Étape 10 Détectez les politiques de façon itérative, en fonction des besoins.

Pour en savoir plus, consultez Réviser les politiques de manière itérative, à la page 481 et les sous-sections.

Étape 11 Lorsque vous êtes prêt, appliquez les politiques.

Vous pouvez appliquer des politiques lorsque vous êtes satisfait du comportement des politiques dans chaque espace de travail.

Vous devez appliquer les politiques à la fois dans l'espace de travail et dans la configuration de l'agent.

Pour en savoir plus, consultez Appliquer des politiques, à la page 558.

Configurer la microsegmentation pour les charges de travail en nuage

Procédure

Étape 1 Installez des agents sur vos charges de travail infonuagique, si nécessaire;

Les connecteurs infonuagique offrent une granularité de niveau VPC/VNet pour la découverte et l'application des politiques. Installez les agents sur des plateformes prises en charge si vous avez besoin de la découverte et de l'application des politiques à un niveau plus granulaire.

Installez les agents en fonction du système d'exploitation sur lequel votre service infonuagique est exécuté. Pour en savoir plus, consultez la section Déployer des agents logiciels.

Étape 2 Configurez des connecteurs infonuagique pour recueillir des étiquettes et des données de flux.

Pour en savoir plus, consultez ;

- Connecteur AWS.
- Connecteur Azure.
- Connecteur GCP

Étape 3 Créez des espaces de travail pour les portées créées par le connecteur.

Pour en savoir plus, consultez Utiliser des espaces de travail pour gérer les politiques.

Étape 4 Découvrir automatiquement les politiques.

Découvrez les politiques pour chaque portée définie par le VPC/VNet et, le cas échéant, pour des portées plus granulaires.

Pour en savoir plus, consultez la section Découvrir automatiquement les politiques.

Étape 5 Examinez et analysez les politiques suggérées.

Consultez Examiner et analyser les politiques, à la page 538 et les sous-sections.

Étape 6 Détectez les politiques de façon itérative, en fonction des besoins.

Consultez Réviser les politiques de manière itérative, à la page 481 et les sous-sections.

Étape 7 Approuvez et appliquez les politiques pour chaque portée.

Vous devez activer l'application dans l'espace de travail concerné et dans le connecteur pour chaque VPC ou VNet, ainsi que pour tous les agents installés sur des charges de travail individuelles.

- Pour en savoir plus, consultez Appliquer des politiques, à la page 558 et les sous-sections.

- Pour en savoir plus :
  - Pour les charges de travail basées sur AWS, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.
  - Pour les charges de travail basées sur Azure, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure.
  - Pour les charges de travail basées sur GCP, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP.

Set Up Microsegmentation for Kubernetes-Based Workloads

Procedure

Étape 1 Install agents on Kubernetes-based workloads.

Be sure to check the requirements and prerequisites.

See Installer les agents Kubernetes ou OpenShift pour une visibilité et une application approfondies.

Agents will automatically be installed on all future workloads managed by the applicable Kubernetes service.

Étape 2 Gather labels for your Kubernetes-based workloads.

Depending on your Kubernetes deployment, see:

- For plain-vanilla Kubernetes and OpenSource workloads:

  Orchestrateurs externes dans Cisco Secure Workload, on page 125 and Kubernetes/OpenShift, on page 144
- For Elastic Kubernetes Services (EKS) Running on Amazon Web Services (AWS):

  Connecteur AWS, on page 241 and Services gérés Kubernetes s'exécutant sur AWS (EKS), on page 253
- For Azure Kubernetes Services (AKS):

  Connecteur Azure, on page 256 and Managed Kubernetes Services Running on Azure (AKS)
- For Google Kubernetes Engine (GKE) running on Google Cloud Platform (GCP):

  Services gérés Kubernetes s'exécutant sur GCP (GKE), on page 273

Étape 3 Create or update your scope tree based on your labels.

See Portées et inventaire.

Étape 4 Create a workspace for each scope for which you want to apply policies.

See Utiliser des espaces de travail pour gérer les politiques.

Étape 5 Automatically discover policies for each low-level scope.

See Découvrir automatiquement les politiques.

Étape 6 (Optional) See applicable additional options under Politiques spécifiques à la plateforme, on page 488.

Étape 7 Review and analyze the suggested policies.

See Examiner et analyser les politiques, on page 538.

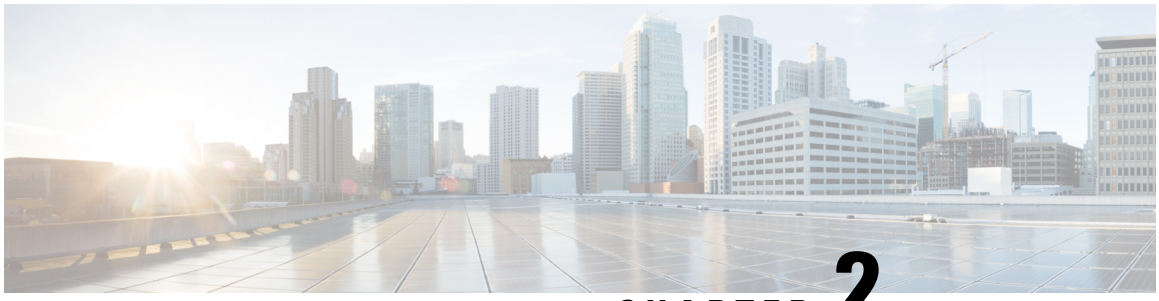
Étape 8 Iteratively discover, review, and analyze policies as needed.

See Réviser les politiques de manière itérative, on page 481.

Étape 9 When you are ready, approve and enforce policies for each scope.

You must enable policy enforcement in the workspace and for the agents.

See Enforce Policies and subtopics, including Application des conteneurs, on page 566.



CHAPTER 2

Cisco Smart Licensing

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. If you have a Cisco Smart Licensing account, you can associate the Cisco Smart Licensing token with a Secure Workload license.

Secure Workload Licenses

- **Tetration workload protection**—For workload protection. License information is available in the **Total workload license usage** table on the **License Usage Information** page.
- **Tetration endpoint visibility**—For workload visibility in Secure Workload. Number of workloads and licenses consumed is available in the **Total endpoint license usage** table on the **License Usage Information** page.
- **Secure Workload PLR**—Purchase the PLR license to use the license reservation PLR mode in Secure Workload.

Registering for Secure Workload Smart Licensing

Table 1: Registering for Secure Workload Smart Licensing

New Users	Existing Users
1. Create a Smart Account on Cisco Software Central and purchase the Secure Workload entitlements. For more information, see Cisco Licensing. 2. Go to Smart Software Manager and create a token to register Secure Workload cluster. 3. From Secure Workload, connect to the Cisco Smart Software Manager (CSSM) portal to register the cluster and sync all the licenses and compliance information, and you can also reserve specific licenses.	1. The purchased Secure Workload entitlements will be saved in the Cisco Smart Software Manager under your Smart Account. To manage, go to Smart Software Manager. 2. Upgrade to Secure Workload release 3.8. 3. Go to Smart Software Manager and create a token to register Secure Workload cluster. 4. From your latest Secure Workload version, connect to the Cisco Smart Software Manager (CSSM) portal to register the cluster and sync all the licenses and compliance information, and you can also reserve specific licenses.

For more information about creating a smart account, see:

- How to Create a Smart Account
- How to Create a Smart Account - Video

Licensing options available in Secure Workload:

- **Connected mode**—The entitlement and compliance information is communicated by Secure Workload with the Smart Software Manager on a periodic basis. If you make changes in the Smart Software Manager, you can refresh the authorization on Secure Workload so the changes immediately take effect. You also can wait for Secure Workload to communicate as scheduled. See Enregistrement des licences Cisco Secure Workload Smart : portail CSSM, on page 10.
- **Air-gapped mode**
  - Smart Software Manager On-Prem—The Smart Software Manager On-Prem allows you to schedule synchronization or manually synchronize Smart License authorization with the Smart Software Manager. To register Secure Workload cluster using Smart Software Manager On-Prem, see Secure Workload Smart License Registration—CSSM On-Prem, on page 17.
  - Specific license reservation—Use license reservation method to reserve licenses from your virtual smart account without accessing the Smart Software Manager or using Smart Software Manager On-Prem. See Réservation de la licence, on page 13.

Note

- Smart licensing is applicable to Secure Workload on-premises version and is not applicable to the SaaS version.
- Smart licensing feature requires Secure Workload cluster running on version 3.8 and later.
- For the data backup and restore feature, smart licenses are required for the primary (active) cluster but not for the standby cluster until it becomes active.
- For Federation clusters, leaders and followers must be individually registered using smart licenses, however, leader will not consume any endpoint or workload licenses.
- The Secure Workload cluster enters non-compliant state when the licenses are being overutilized or the licenses have expired. It is recommended that you take action immediately to restore the cluster in compliant state. In release 3.8, no features are affected due to the non-compliant state.

- Enregistrement des licences Cisco Secure Workload Smart : portail CSSM, on page 10
- Réservation de la licence, on page 13
- Secure Workload Smart License Registration—CSSM On-Prem, on page 17
- Synchroniser les licences Smart, on page 18

Enregistrement des licences Cisco Secure Workload Smart : portail CSSM

Before you begin

Assurez-vous que :

- La connectivité Internet est disponible pour enregistrer la grappe Cisco Secure Workload auprès du portail CSSM.
- Le compte Smart Licensing contient les licences disponibles dont vous avez besoin.

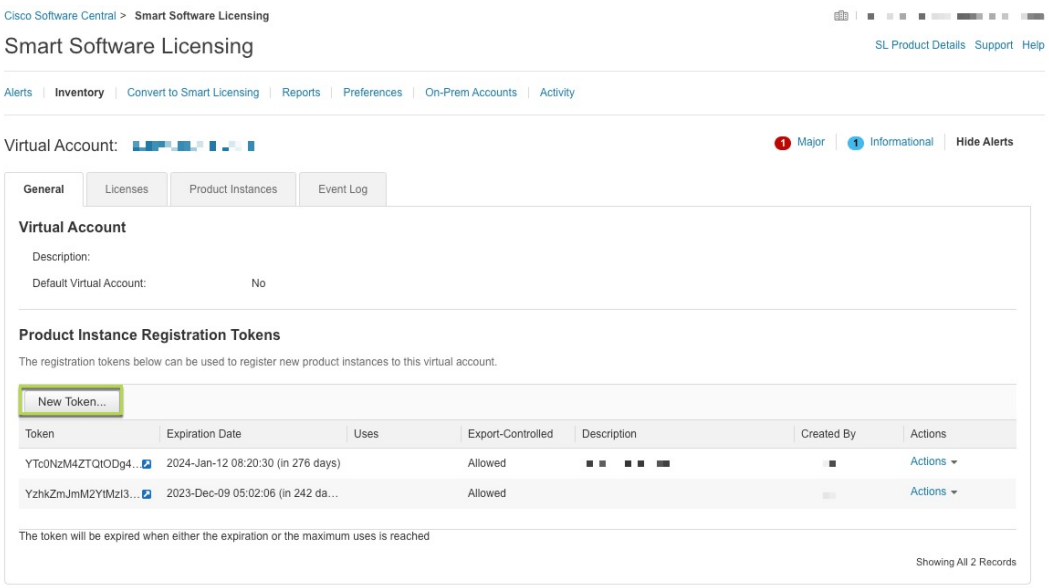
Procedure

Étape 1 Rendez-vous sur le portail Cisco Smart Software Manager (CSSM) et effectuez les actions suivantes pour générer un jeton pour le compte virtuel dans lequel vous souhaitez enregistrer la grappe Cisco Secure Workload.

a) Connectez-vous au portail CSSM.

b) Choisissez le compte virtuel approprié, accédez à **Smart Software Licensing** > **General(Généralités)** et cliquez sur **New Token** (Nouveau jeton). Suivez les instructions à l'écran pour créer un jeton.

Figure 1: Créer un nouveau jeton sur le portail CSSM

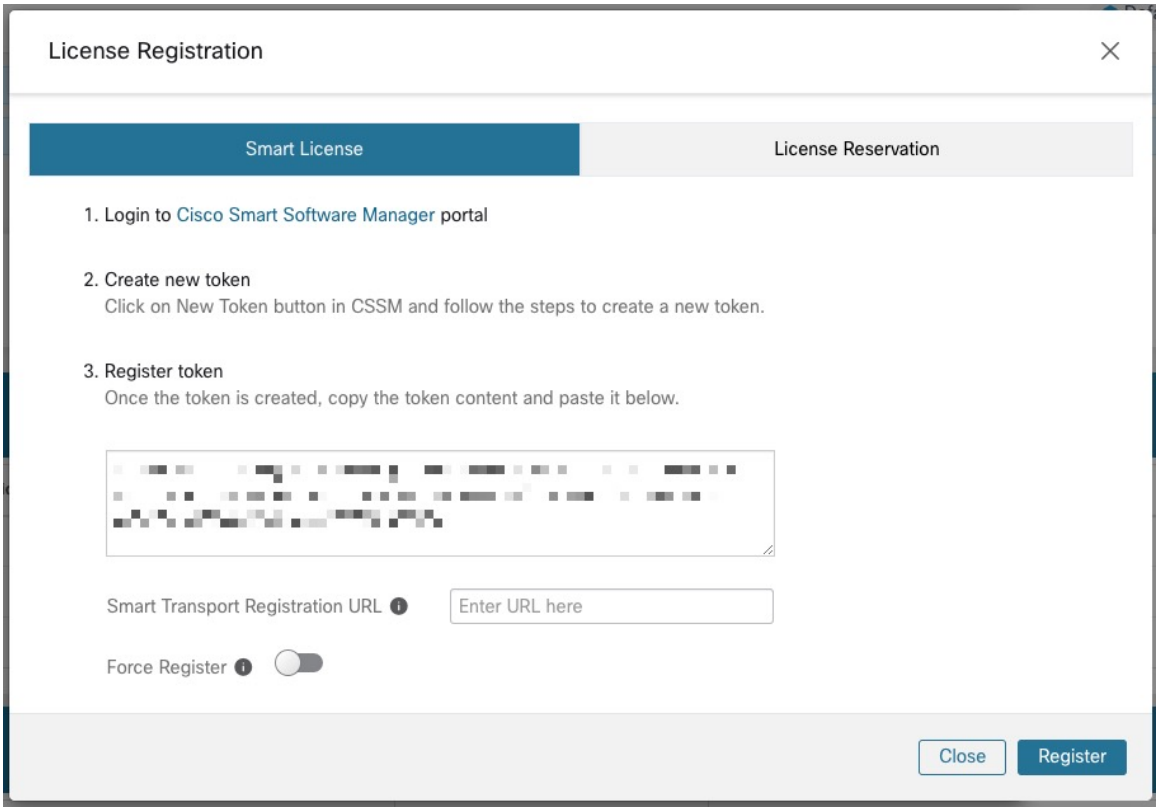


c) Copiez le jeton généré.

Étape 2 Dans Cisco Secure Workload, accédez à **Manage (Gestion)** > **Service Settings(Paramètres de service)** > **Licenses (Licences)**, puis cliquez sur **Register (Enregistrer)**.

Étape 3 Sous l'onglet **Smart Licenses** (Licences Smart), saisissez le jeton généré à partir du portail CSSM.

Figure 2: Page d'enregistrement de la licence Smart pour Cisco Secure Workload



Étape 4 (Facultatif) Activez **Force Register** (Forcer l'enregistrement) pour poursuivre l'enregistrement même si l'UUID de la grappe est déjà enregistré auprès de CSSM.

Étape 5 Cliquez sur **Register** (Inscrire).

L'enregistrement de Cisco Secure Workload auprès du portail du CSSM est lancé. Pour afficher l'état mis à jour de l'enregistrement, actualisez la page **License Usage Information** (renseignements sur l'utilisation des licences).

Annulation de l'enregistrement des licences Smart Cisco Secure Workload

Procedure

Étape 1 Dans la page **License Usage Information** (Informations d'utilisation des licences), cliquez sur **Deregister** (Désinscrire).

Étape 2 Pour confirmer, cliquez sur **Yes** (Oui).

Après avoir actualisé la page **d'informations sur l'utilisation des licences**, le champ **État de la licence** affiche l'état de la licence comme **Non enregistré** et la grappe entre dans la période d'évaluation.

Réservation de la licence

La fonctionnalité de réservation de licences est utilisée pour déployer les licences Smart dans un réseau isolé. Avant de commencer, assurez-vous que les licences requises pour Cisco Secure Workload sont disponibles dans votre compte Smart. Pour connaître le nombre de licences disponibles dans votre compte, accédez au portail des licences logicielles CSSM Smart et cliquez sur **Inventory (Inventaire)** > **Licenses (Licences).**

Procedure

Étape 1 Sur l'interface utilisateur de Cisco Secure Workload, accédez à **Manage** > **Service Settings** > **Licenses**. La page **License Usage Information** (Informations sur l'utilisation des licences) s'affiche.

Étape 2 Cliquez sur **Register** (Inscrire).

Étape 3 Sélectionnez l'onglet **License Reservation** (réservation de licence), puis cliquez sur **Yes** (oui) pour confirmer. Un code de demande est généré par Cisco Secure Workload.

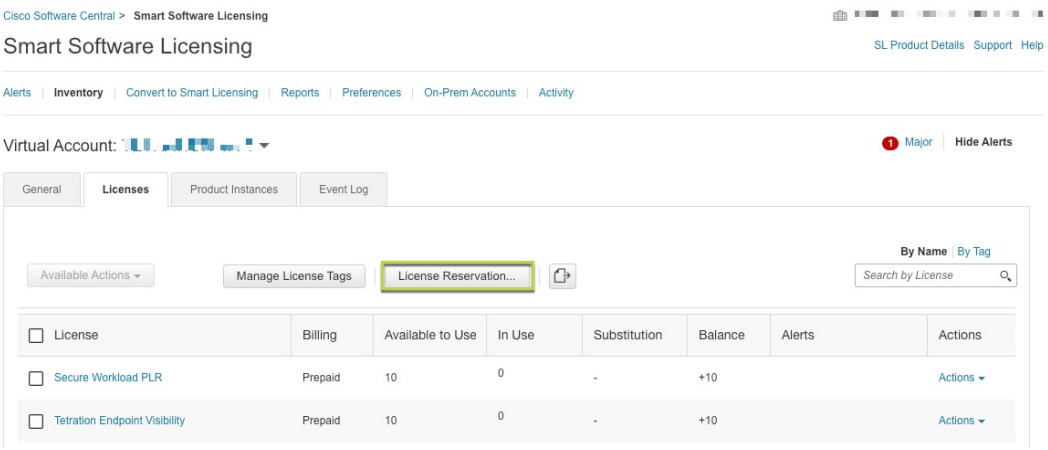
Étape 4 Copiez le code de demande généré.

Étape 5 Accédez au portail de licences logicielles CSSM Smart et effectuez les actions suivantes :

a) Accédez à **Inventory (Inventaire)** > **Licenses (Licences)**.

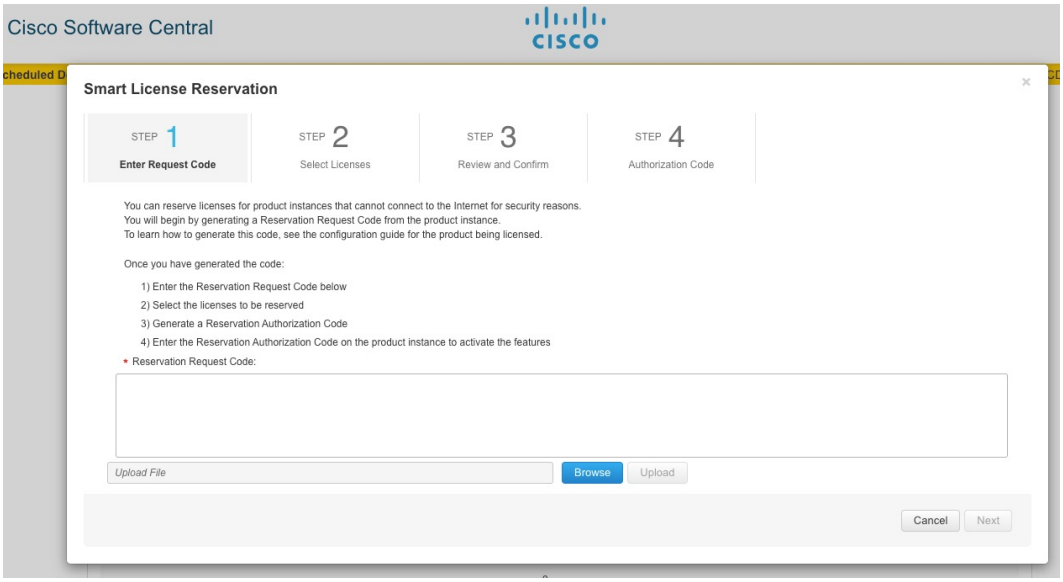
b) Cliquez sur **License Reservation**(Réservation de licence), puis cliquez sur **Proceed** (continuer) pour continuer.

Figure 3: Page des licences - Portail CSSM



c) Saisissez le code de demande généré par Cisco Secure Workload, puis cliquez sur **Next**(suivant).

Figure 4: Réservation de licences – Portail CSSM



d) Sous **Licenses to Reserve** (Licences à réserver), choisissez l'une des options suivantes et cliquez sur **Next**(suivant).

- Cisco Secure Workload PLR : aucune limitation sur le nombre de charges de travail et de points terminaux qui peuvent être configurés sur la grappe.
- Réservation d'une licence précise : en fonction des licences de charge de travail et de points terminaux achetées, mettre à jour le nombre de réservations pour les types de licence Tetration Workload Protection et Tetration Endpoint Visibility.

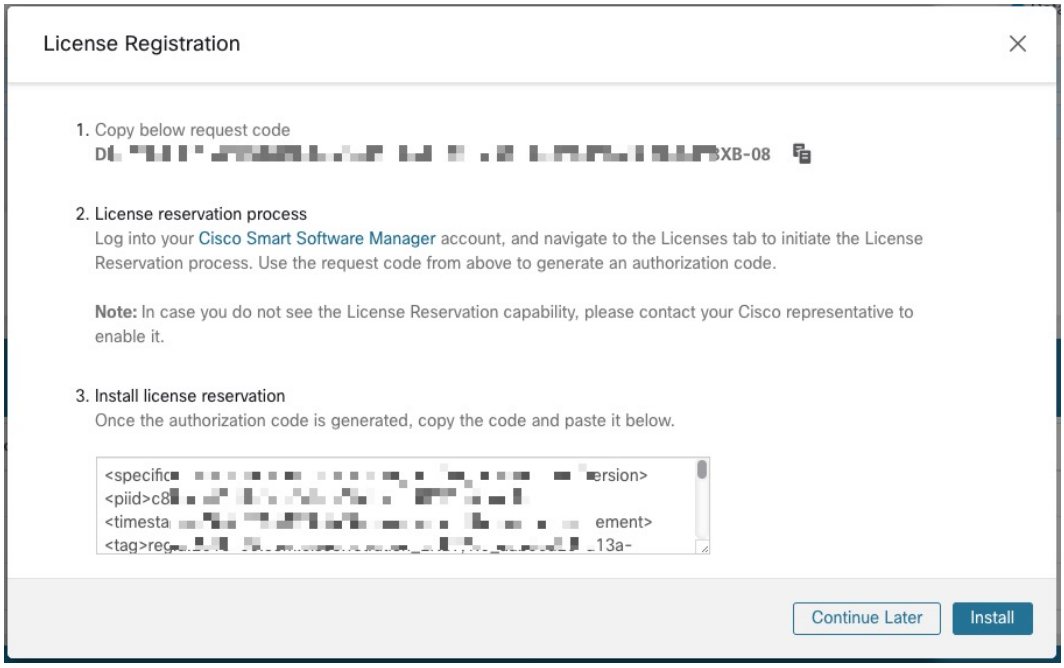
e) Passez en revue le type de licence sélectionné et la quantité de licences à réserver, puis cliquez sur **Generate Authorization Code** (générer un code d'autorisation).

f) Cliquez sur **Copy to Clipboard** (Copier dans le presse-papiers).

g) Cliquez sur **Close** (Fermer) pour quitter l'assistant.

Étape 6 Dans Cisco Secure Workload, saisissez le code d'autorisation et cliquez sur **Install** Installer).

Figure 5: Page de réservation de licences Cisco Secure Workload



Sur le portail CSSM, les licences réservées peuvent être consultées sous l'onglet **Licenses** (Licences).

Note

- Pendant le processus de réservation de licences, vous pouvez également sélectionner **Continue Later** (Continuer plus tard). Pour reprendre le processus de réservation, dans la page **License Usage Information** (d'informations d'utilisation de la licence), cliquez sur **Continue Reservation** (Poursuivre la réservation).
- Si vous décidez d'annuler la réservation de licence, cliquez sur **Cancel Reservation** (Annuler la réservation) dans la page **d'informations sur l'utilisation des licences** et effectuez l'une des actions suivantes :
  - Lorsque vous générez un code d'autorisation, une licence est généralement réservée pour une utilisation sur CSSM. Pour renvoyer la licence, saisissez le code d'autorisation généré à partir du CSSM. Cisco Secure Workload génère un code de retour qui doit être saisi dans CSSM.
  - Si vous n'avez pas de licence sur CSSM, sélectionnez l'onglet **I do not have a license in CSSM** (Je n'ai pas de licence sur CSSM).

Mettre à jour la réservation d'une licence spécifique

Procedure

Étape 1 Sur le portail CSSM, procédez comme suit :

a) Pour la licence spécifique réservée, dans le menu déroulant **Actions** (actions), choisissez **Update Reserved Licenses**(mettre à jour les licences réservées).
b) Choisissez **Reserve a specific License** (Réserver une licence spécifique) et mettez à jour le nombre de réservations pour les types de licence Tetration Workload Protection et Tetration Endpoint Visibility requis.
c) Cliquez sur **Next** (suivant).
d) Passez en revue les réservations sélectionnées et cliquez sur **Generate Authorization Code** (générer un code d'autorisation).
e) Cliquez sur **Copy to Clipboard** (Copier dans le presse-papiers).

Étape 2 Dans Cisco Secure Workload, procédez comme suit pour mettre à jour la réservation de licences spécifiques :

a) Dans la page **des informations sur l'utilisation des licences**, cliquez sur **Update Reservation** (Mettre à jour les réservations).
b) Saisissez le code d'autorisation du CSSM.
c) Cliquez sur **Generate Confirmation Code** (Générer un code de confirmation).
d) Copiez le code de confirmation généré et cliquez sur **Next**(suivant).
e) Le code de confirmation généré ne peut pas être récupéré ultérieurement dans Cisco Secure Workload. Assurez-vous de copier le code reçu en retour. Cliquez sur l'icône **Copy** (Copier).

Étape 3 Sur le portail CSSM, procédez comme suit pour terminer le processus de réservation :

a) Sous **Product Instances**(instances de produit), choisissez la licence à réserver et cliquez sur **Actions**(actions).
b) Sélectionnez **Enter Confirmation Code** (Saisir le code de confirmation).
c) Saisissez le code de confirmation et cliquez sur **OK**.

Étape 4 Dans Cisco Secure Workload, cliquez sur **Finish** (Terminer) pour quitter l'assistant.

Actualisez la page **License Usage Information** (informations sur l'utilisation des licences) pour afficher les détails de la réservation de licence mis à jour.

Reprise de la réservation de licences spécifiques

Procedure

Étape 1 Dans Cisco Secure Workload, dans la page **License Usage Information** (informations d'utilisation de la licence), cliquez sur **Deregister** (Désinscrire).

Étape 2 Pour générer un code de retour, cliquez sur **Generate return code** (Générer le code de retour).

Étape 3 Cliquez sur l'icône **Copy** (Copier) pour copier le code retour et cliquez sur **Next** (Suivant). Assurez-vous de copier le code de retour généré, car vous ne pourrez pas le récupérer plus tard.

Étape 4 Pour terminer le processus de désinscription, accédez au portail CSSM et effectuez les étapes suivantes :

a) Sous **Product Instances**(instances de produit), choisissez la licence à annuler et cliquez sur **Actions**(actions).
b) Choisissez **Remove** (Supprimer).
c) Saisissez le code de retour et cliquez sur **Remove Reservation** (Supprimer la réservation).

Étape 5 Dans Cisco Secure Workload, cliquez sur **Finish** (Terminer) pour quitter l'assistant.

Les licences réservées sont retournées au compte Smart. Cisco Secure Workload passe en période d'évaluation et les licences réservées sont classées dans l'état de conformité Non enregistré.

Secure Workload Smart License Registration—CSSM On-Prem

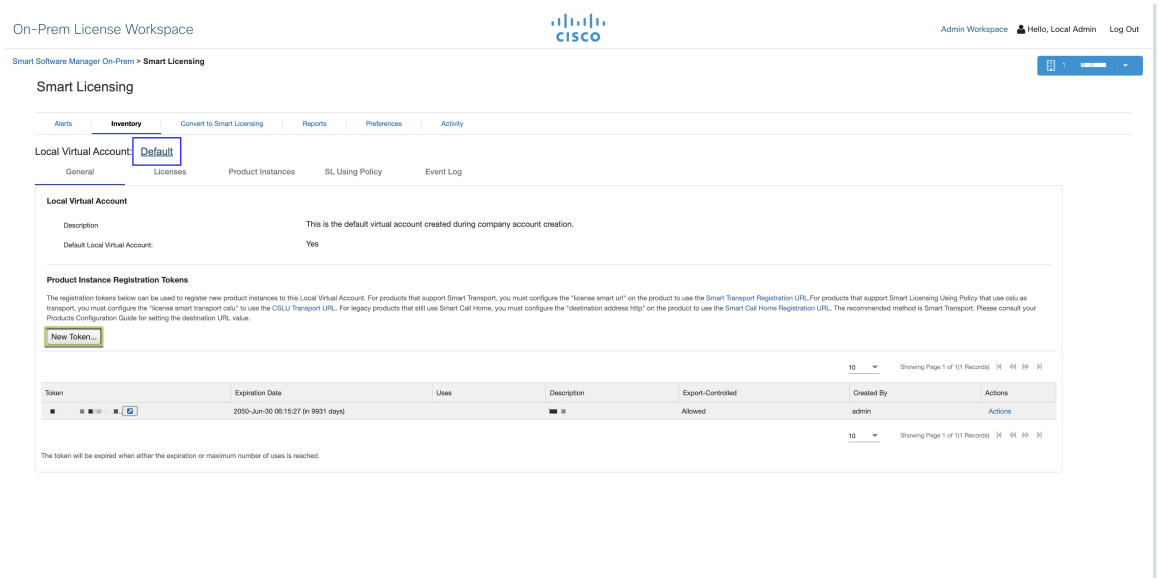
The Smart Software Manager On-Prem allows you to schedule synchronization of licenses or provides an option to manually synchronize Smart License authorizations with the Smart Software Manager portal. You can use CSSM on-prem to register Secure Workload in air-gapped networks or if you prefer to manage smart licenses through a single connection from your network.

Procedure

Étape 1 Set up Smart Software Manager On-prem. For more information, see Cisco Software Central.

Étape 2 Log in to the Smart Software Manager On-prem and select the virtual account. Under the **General** tab, click **New Token**. Follow the onscreen instructions to create a token.

Figure 6: On-Prem License Workspace



Étape 3 In Secure Workload, navigate to **Manage** > **Service Settings** > **Licenses**, and then click **Register**.

Étape 4 Under the **Smart Licenses** tab, enter the generated token from the Smart Software Manager On-prem.

Étape 5 Under the **Smart Licenses** tab, in the **Smart Transport Registration URL** field, enter the Smart Transport Registration URL of your Smart Software Manager On-Prem.

Étape 6 (Optional) Enable **Force Register** to continue with the registration even if the cluster UUID is already registered with CSSM.

Étape 7 Click **Register**.

The registration of Secure Workload with the CSSM on-prem is initiated. To view the updated status of the registration, refresh the **License Usage Information** page. Synchronize Smart Software Manager On-Prem to the Smart Software Manager portal after assigning the licenses.

Synchroniser les licences Smart

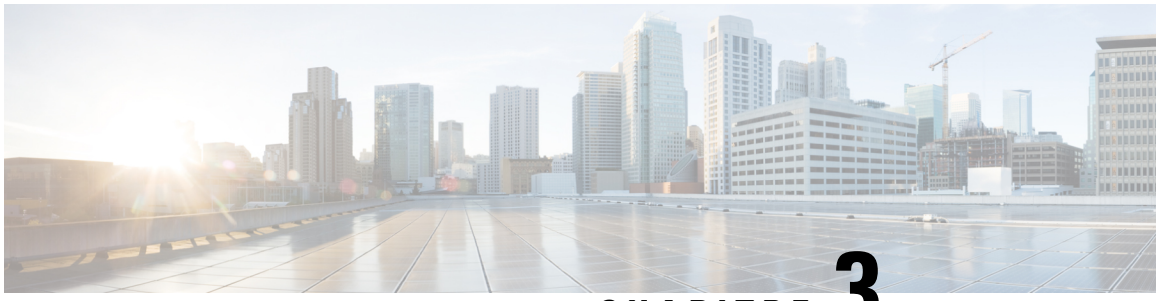
Les renseignements relatifs aux licences et à la conformité sont synchronisés avec le portail Smart Software Manager toutes les 24 heures. Cependant, si la grappe n'est pas conforme et que les licences sont renouvelées sur le CSSM, vous pouvez mettre à jour manuellement les licences en vous connectant au portail CSSM directement ou par l'intermédiaire de Smart Software Manager On-prem en procédant comme suit :

Procedure

Étape 1 Dans la page **License Usage Information** (Informations sur l'utilisation des licences), cliquez sur **Renew Operations (Renouveler le fonctionnement)** > **Renew Authorization (Renouveler l'autorisation)**.

Étape 2 Pour confirmer, cliquez sur **Yes** (Oui).

Après avoir actualisé la page **License Usage Information** (d'informations d'utilisation des licences), vous pouvez afficher les licences mises à jour ainsi que la date et l'heure de la dernière synchronisation réussie avec le CSSM.



CHAPITRE 3

Déployer des agents logiciels sur les charges de travail

Un agent logiciel Cisco Secure Workload est un logiciel léger que vous installez sur vos charges de travail. Le but de l'agent est de :

- Recueillir des renseignements sur l'hôte tels que les interfaces réseau et les processus actifs en cours d'exécution dans le système.
- Surveiller et recueillir des renseignements sur les flux du réseau.
- Appliquer les politiques de sécurité en définissant des règles de pare-feu pour les hôtes sur lesquels l'agent logiciel est installé et activé.

Les agents mettent automatiquement à jour l'inventaire de la charge de travail sécurisée lorsque les adresses d'interface changent. Vous n'avez pas besoin d'installer les agents sur les ordinateurs des utilisateurs finaux (employés).

Déployer des agents logiciels

Note Les scripts du programme d'installation téléchargés à partir de comptes LDAP ou AD avec le mappage automatique des rôles échouent une fois que vous êtes déconnecté. Pour donner aux scripts du programme d'installation un accès ininterrompu à la grappe, activez Use Local Authentication (utiliser l'authentification locale).

Lors du déploiement, l'agent se voit attribuer une identité unique par la grappe Cisco Secure Workload en fonction d'un ensemble de paramètres propres à l'hôte sur lequel l'agent est exécuté. Si le nom d'hôte et l'UUID du BIOS font partie de l'ensemble de paramètres, vous pourriez rencontrer les problèmes suivants :

1. Échec de l'enregistrement lors du clonage d'une machine virtuelle en conservant l'UUID BIOS et le nom d'hôte, et lors du clonage instantané d'un VDI. L'échec de l'enregistrement se produit parce que Cisco Secure Workload comporte déjà un agent logiciel enregistré qui utilise les mêmes paramètres définis. Vous pouvez supprimer l'agent enregistré à l'aide d'OpenAPI. Dans certains cas, un UUID BIOS en double configuré lors du démarrage est modifié par VMware après un certain temps. L'inscription de l'agent est rétablie une fois que les services Cisco Cisco Secure Workload sont redémarrés.
2. Une nouvelle identité est générée pour l'agent si le nom d'hôte est modifié et l'hôte redémarré. L'agent redondant ou l'ancien agent est marqué comme inactif après un certain temps. Pour en savoir plus, consultez la section Foire aux questions.

Supported Platforms and Requirements

For supported platforms and additional requirements for software agents, see:

- The release notes for your release, see Release Notes.
- The agent install wizard in the Secure Workload web portal: In the navigation bar on the left, choose **Manage** > **Agents**, then click the **Installer** tab. Choose an installation method, a platform, and if applicable, an agent type to see supported platform versions.
- For additional dependencies, see Support Matrix. Ensure that you are seeing all the columns.
- Additional requirements for each platform and agent type are listed in the following sections.

Installation des agents Linux pour une visibilité approfondie et une application

Configuration requise et conditions préalables à l'installation des agents Solaris

- Consultez la section Supported Platforms and Requirements.
- Privilèges racine pour installer et exécuter les services.
- Espace de stockage de 1 Go pour l'agent et le fichier journal.

- Des exclusions de sécurité sont configurées sur les applications de sécurité qui surveillent l'hôte pour empêcher ces applications de bloquer l'installation ou l'activité des agents. Pour en savoir plus, consultez Exclusions de sécurité.
- Un utilisateur spécial, **tet-sensor**, est créé sur l'hôte sur lequel l'agent est installé. Si PAM ou SELinux est configuré sur l'hôte, l'utilisateur tet-sensor doit recevoir les privilèges appropriés pour exécuter le processus tet-sensor et établir des connexions avec les collecteurs. Si un autre répertoire d'installation est fourni et que SELinux est configuré, assurez-vous que l'exécution est autorisée pour cet emplacement.
- Vous devez être en mesure d'utiliser la commande unzip si l'agent est installé à l'aide de la méthode d'installation automatique (script d'installation).

Méthodes prises en charge pour l'installation des agents Linux

Méthodes d'installation d'un agent Linux pour une visibilité et une application approfondies :

- Installer l'agent Linux à l'aide de la méthode du programme d'installation du script de l'agent, on page 22
    - Prise en charge des agents pour la plateforme de mise en réseau Blufield de NVIDIA
- Installer l'agent Linux à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 21

Installer l'agent Linux à l'aide de la méthode du programme d'installation de l'image de l'agent

Nous vous recommandons d'utiliser la méthode du script d'installation automatisé pour installer les agents Linux. Utilisez la méthode de l'installation par image si vous avez une raison précise d'utiliser cette méthode manuelle.

Prérequis

Configurez ACTIVATION_Key et HTTPS_PROXY dans le fichier user.cfg pour les grappes de logiciels-services et lorsque vous installez l'agent sur un détenteur autre que par défaut, des grappes sur site à plusieurs détenteurs. Pour en savoir plus, consultez (installations manuelles seulement) Mettre à jour le fichier de configuration utilisateur.

Pour installer un agent Linux à l'aide de la méthode de l'image de l'agent :

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(gestion des agents), puis sélectionnez l'onglet **Installer** (Programme d'installation).

Étape 2 Cliquez sur **Agent Image Installer** (Programme d'installation de l'image de l'agent).

Étape 3 Dans le champ **Platform** (plateforme), saisissez Linux.

Étape 4 Saisissez le type et la version de l'agent requis, puis, à partir des résultats, téléchargez la version de l'agent nécessaire.

Étape 5 Copiez le paquet logiciel RPM sur tous les hôtes Linux pour le déploiement.

Note Si l'agent est déjà installé sur l'hôte, ne le réinstallez pas. Pour mettre à niveau l'agent, consultez la section Mise à niveau des agents logiciels.

Étape 6 En fonction de votre plateforme, exécutez les commandes RPM avec les privilèges racine.

- Pour les plateformes RHEL/CentOS/Oracle, exécutez la commande : `rpm -ivh <rpm_filename>`
- Pour la plateforme Ubuntu :
  - Pour récupérer la liste des dépendances et vous assurer que toutes les dépendances sont respectées, exécutez la commande : `rpm -qpR <rpm_filename>`
  - Installez l'agent à l'aide de l'option « –nodeps » en exécutant la commande : `rpm -ivh \\--nodeps <rpm filename>`

Installer l'agent Linux à l'aide de la méthode du programme d'installation du script de l'agent

Nous vous recommandons d'utiliser la méthode du script du programme d'installation pour déployer des agents Linux afin d'assurer la visibilité approfondie et l'application.

Note

- L'agent Linux installé prend en charge la visibilité approfondie et l'application.
- Le paramètre par défaut est Disabled (désactivé). Pour activer l'application, consultez Creating an Agent Config Profile.

Pour installer un agent Linux à l'aide du programme d'installation de script :

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de **démarrage rapide** et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Script Installer** (Installateur de script d'agent).

Étape 3 Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez **Linux**.

Pour afficher les plateformes Linux prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).

Étape 4 Choisissez le détenteur pour installer les agents.

Note Les grappes de logiciel-service Cisco Secure Workload ne nécessitent pas la sélection de détenteur.

Étape 5 Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.

Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont automatiquement attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :

- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
- Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.

Étape 6 Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(oui), puis saisissez une URL de serveur mandataire valide.

Étape 7 Dans la section **Installer expiration** (Expiration de la validité du programme d'installation), sélectionnez une option :

- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
- Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
- Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
- Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.

Étape 8 Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

Étape 9 Copiez le script d'interface Shell du programme d'installation sur les hôtes Linux et exécutez la commande suivante pour accorder l'autorisation d'exécution au script : `chmod u+x tetration_installer_default_sensor_linux.sh`

Note Le nom du script peut différer selon le type d'agent et la portée sélectionnés.

Étape 10 Pour installer l'agent, exécutez la commande suivante avec les privilèges de l'utilisateur racine : `./tetration_installer_default_sensor_linux.sh`

Note Si un agent est déjà installé sur le détenteur, vous ne pouvez pas poursuivre l'installation.

Nous vous recommandons d'exécuter la vérification préalable, comme spécifié dans les détails d'utilisation du script.

Détails d'utilisation du script d'installation de Linux :

```
bash tetration_linux_installer.sh [--pre-check] [--skip-pre-check=<option>] [--no-install]
 [--logfile=<filename>] [--proxy=<proxy_string>] [--no-proxy] [--help] [--version]
[--sensor-version=<version_info>] [--ls] [--file=<filename>] [--save=<filename>] [--new]
[--reinstall] [--unpriv-user] [--force-upgrade] [--upgrade-local]
[--upgrade-by-uuid=<filename>] [--basedir=<basedir>] [--logbasedir=<logbdir>]
[--tmpdir=<tmp_dir>] [--visibility] [--golden-image]
  --pre-check: run pre-check only
  --skip-pre-check=<option>: skip pre-installation check by given option; Valid options
include 'all', 'ipv6' and 'enforcement'; e.g.: '--skip-pre-check=all' will skip all
pre-installation checks; All pre-checks will be performed by default
  --no-install: will not download and install sensor package onto the system
```

```
  --logfile=<filename>: write the log to the file specified by <filename>
  --proxy=<proxy_string>: set the value of CL_HTTPS_PROXY, the string should be formatted
as http://<proxy>:<port>
  --no-proxy: bypass system wide proxy; this flag will be ignored if --proxy flag was
provided
  --help: print this usage
  --version: print current script's version
  --sensor-version=<version_info>: select sensor's version; e.g.: '--sensor-version=3.4.1.0';
 will download the latest version by default if this flag was not provided
  --ls: list all available sensor versions for your system (will not list pre-3.1 packages);
 will not download any package
  --file=<filename>: provide local zip file to install sensor instead of downloading it
from cluster
  --save=<filename>: download and save zip file as <filename>
  --new: remove any previous installed sensor; previous sensor identity has to be removed
from cluster in order for the new registration to succeed
  --reinstall: reinstall sensor and retain the same identity with cluster; this flag has
higher priority than --new
  --unpriv-user=<username>: use <username> for unpriv processes instead of tet-sensor
  --force-upgrade: force sensor upgrade to version given by --sensor-version flag; e.g.:
'--sensor-version=3.4.1.0 --force-upgrade'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-local: trigger local sensor upgrade to version given by --sensor-version flag:
 e.g.: '--sensor-version=3.4.1.0 --upgrade-local'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-by-uuid=<filename>: trigger sensor whose uuid is listed in <filename> upgrade
to version given by --sensor-version flag; e.g.: '--sensor-version=3.4.1.0
--upgrade-by-uuid=/usr/local/tet/sensor_id'; apply the latest version by default if
--sensor-version flag was not provided
  --basedir=<base_dir>: instead of using /usr/local use <base_dir> to install agent. The
full path will be <base_dir>/tetration
  --logbasedir=<log_base_dir>: instead of logging to /usr/local/tet/log use <log_base_dir>.
 The full path will be <log_base_dir>/tetration
  --tmpdir=<tmp_dir>: instead of using /tmp use <tmp_dir> as temp directory
  --visibility: install deep visibility agent only; --reinstall would overwrite this flag
if previous installed agent type was enforcer
  --golden-image: install Cisco Secure Workload Agent but do not start the Cisco Secure
Workload Services; use to install Cisco Secure Workload Agent on Golden Images in VDI
environment or Template VM. On VDI/VM instance created from golden image with different
host name, Cisco Secure Workload Services will work normally
```

Note

- Ubuntu utilise le paquet natif .deb, et les nouvelles installations et réinstallations utilisent ce type de paquet. Les mises à niveau des versions précédentes se poursuivent avec le paquet .rPM.
- Le paquet Ubuntu .deb est installé sous `/opt/cisco/tetration`.
- Il n'y a pas de prise en charge à la relocalisation pour le paquet .deb et l'option –basedir n'est pas prise en charge pour Ubuntu.

Prise en charge des agents pour la plateforme de mise en réseau Blufield de NVIDIA

Une unité de traitement des données (DPU) est un processeur programmable conçu pour gérer des tâches centrées sur les données, notamment le transfert de données, l'optimisation de la consommation d'énergie, la sécurité, la compression, l'analyse et le chiffrement.

L'unité de traitement de données (DPU) de NVIDIA est une carte d'interface réseau Smart (SmartNic) offrant des rendements réseau intéressants. Elle offre une capacité de carte réseau Ethernet NIC haut débit. Notamment,

elle permet l'exécution de logiciels directement sur la carte NIC elle-même, ce qui permet l'interception, la surveillance ou la manipulation du trafic réseau passant par la NIC.

NVIDIA facilite cette fonctionnalité en fournissant le SDK DOCA. S'appuyant sur la technologie de virtualisation basée sur la virtualisation PCIe Single Root I/O (SR-IOV), la DPU établit un mécanisme permettant aux machines virtuelles (VM) de communiquer directement sans l'intervention de l'hyperviseur. La DPU intègre un commutateur électronique eSwitch à accélération matérielle basé sur OpenVSwitch pour le contrôle du réseau, ce qui améliore l'efficacité globale.

Exigences et prérequis

- Assurez-vous que DOCA basé sur Ubuntu 22.04 est installé sur la plateforme de réseau BlueField.
- Configurez le réseau de la carte DPU pour permettre la connexion de l'agent à la grappe par l'intermédiaire de l'une des interfaces hors bande. Les options incluent oob_net0, tmfifo_net0 ou la connexion dans la bande par enp3s0f0s0.

Installation des agents

L'installation suit un processus de type Linux.

1. Accédez à Méthodes d'installation des agents :
   - Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur Install Agents (Installer les agents).
   - Dans le volet de navigation, choisissez **Manage (Gestion)**> **Workloads (Charges de travail)**> **Agents (Agents)**.
2. Dans l'onglet **Installer** (Programme d'installation), sélectionnez **Agent Script Installer** (Programme d'installation de script d'agent).
3. Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez **Linux**.

   Pour afficher les plateformes Linux prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).

Note L'agent Cisco Secure Workload est uniquement pris en charge sur le SDK DOCA basé sur Ubuntu 22.

4. Choisissez le détenteur pour installer les agents.

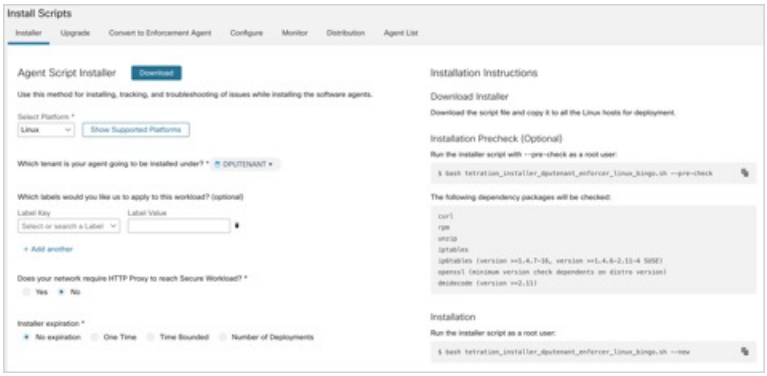
Note La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.

5. Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.
6. Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(oui), puis saisissez un serveur mandataire valide.
7. Dans la section **Installer expiration** (expiration du programme d'installation), sélectionnez-en une option parmi celles disponibles :

- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
- Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
- Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
- Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.

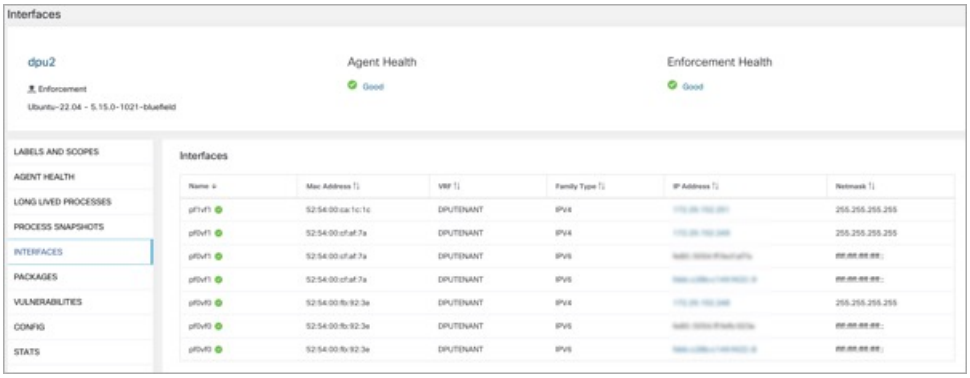
8. Cliquez sur **Download** (Télécharger) pour télécharger le script d'installation de Linux sur la DPU à l'aide de l'un de ses périphériques réseau.
9. Exécutez le script d'installation. Pour en savoir plus, consultez Installer l'agent Linux à l'aide de la méthode du programme d'installation du script de l'agent.

Figure 7: Script d'installation



Accédez à **Software Agents (Agents logiciels)** > **Agent List (Liste d'agents)** et cliquez sur un **nom d'hôte**. Sous **Interfaces**, vous pouvez afficher le mappage actuel des interfaces avec les adresses IP associées.

Figure 8: Mappage d'interface



Accédez à **Investigate** > **Traffic** (Enquêter sur le trafic) pour surveiller le trafic réseau entre les machines virtuelles (VM) lorsque celles-ci utilisent les interfaces de réseau virtuelles SR_IOV fournies par la DPU. L'agent sur la DPU permet la segmentation du trafic réseau entre ces interfaces réseau virtuelles.

Vérifier l'installation de l'agent Linux

Procedure

Exécutez la commande sudo rpm -q tet-sensor `sudo rpm -q tet-sensor`.

```
sudo rpm -q tet-sensor
```

Une seule entrée en sortie confirme qu'un agent Linux est installé sur l'hôte.

Exemple de résulta : `tet-sensor-3.1.1.50-1.el6.x86_64`

La sortie spécifique peut différer en fonction de la plateforme et de l'architecture.

Installation des agents Windows pour une visibilité approfondie et pour application

Exigences et conditions préalables à l'installation de l'agent Windows

- Consultez la section Plateformes prises en charge et exigences.
- Des privilèges d'administrateur sont requis pour l'installation et l'exécution du service.
- Npcap doit être installé sur les charges de travail exécutant Windows 2008 R2 ou lorsque la version de l'agent installé est antérieure à la version 3.8. Si le pilote Npcap n'est pas déjà installé, la version Npcap recommandée est installée en arrière-plan par l'agent après le démarrage du service. Pour en savoir plus, consultez les informations de version de Npcap.
- Un Go d'espace de stockage pour les fichiers des agents et des journaux.
- Activez les services Windows requis pour l'installation de l'agent. Certains des services Windows auraient pu être désactivés si vos hôtes Windows avaient été renforcés en matière de sécurité ou s'ils ont changé par rapport aux configurations par défaut. Pour en savoir plus, consultez la section Services Windows requis.
- Les exclusions de sécurité configurées sur les applications de sécurité qui surveillent l'hôte et qui pourraient bloquer l'installation de l'agent ou son activité. Pour en savoir plus, consultez Exclusions de sécurité.

Méthodes prises en charge pour l'installation des agents Windows

Il existe deux méthodes pour installer les agents Windows pour une visibilité approfondie et la mise en application.

- Installer l'agent Windows à l'aide de la méthode du programme d'installation du script de l'agent, on page 28
- Installer l'agent Windows à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 30

Vous pouvez également les installer en utilisant une image Golden. Pour en savoir plus, consultez la section Déploiement des agents sur une instance VDI ou un modèle de machine virtuelle (Windows)

Installer l'agent Windows à l'aide de la méthode du programme d'installation du script de l'agent

Nous vous recommandons d'utiliser la méthode du programme d'installation de scripts pour déployer les agents Windows afin d'obtenir une visibilité et une application approfondies.

Note

- L'agent Windows installé prend en charge la visibilité approfondie et la mise en application.
- Le paramètre par défaut est Disabled (désactivé). Pour activer l'application, consultez Creating an Agent Config Profile, on page 83.

Pour installer un agent Windows à l'aide du programme d'installation de script :

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Script Installer** (Installateur de script d'agent).

Étape 3 Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez **Windows**.

Pour afficher les plateformes Windows prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).

Étape 4 Choisissez le détenteur pour installer les agents.

Note La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.

Étape 5 Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.

Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :

- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
- Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.

Étape 6 Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.

Étape 7 Dans la section **Installer expiration** (Expiration de la validité de l'installateur), sélectionnez une option parmi celles disponibles :

- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
- Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
- Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
- Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.

Étape 8 Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

Étape 9 Copiez le script d'installation PowerShell sur tous les hôtes Windows pour le déploiement et exécutez le script avec des privilèges d'administration.

Note
- Selon les paramètres du système, il peut être nécessaire d'exécuter la commande `Unblock-File` avant d'autres commandes.
- Le script ne s'exécute pas si l'agent est déjà installé sur le détenteur.

Nous vous recommandons d'exécuter la vérification préalable, comme spécifié dans les détails d'utilisation du script.

Détails d'utilisation du script d'installation de Windows :

```
# powershell -ExecutionPolicy Bypass -File tetration_windows_installer.ps1 [-preCheck]
[-skipPreCheck <Option>] [-noInstall] [-logFile <FileName>] [-proxy <ProxyString>] [-noProxy]
 [-help] [-version] [-sensorVersion <VersionInfo>] [-ls] [-file <FileName>] [-save <FileName>]
 [-new] [-reinstall] [
-npcap] [-forceUpgrade] [-upgradeLocal] [-upgradeByUUID <FileName>] [-visibility]
[-goldenImage] [-installFolder <Installation Path>]
  -preCheck: run pre-check only
  -skipPreCheck <Option>: skip pre-installation check by given option; Valid options include
 'all', 'ipv6' and 'enforcement'; e.g.: '-skipPreCheck all' will skip all pre-installation
 checks; All pre-checks will be performed by default
  -noInstall: will not download and install sensor package onto the system
  -logFile <FileName>: write the log to the file specified by <FileName>
  -proxy <ProxyString>: set the value of HTTPS_PROXY, the string should be formatted as
http://<proxy>:<port>
  -noProxy: bypass system wide proxy; this flag will be ignored if -proxy flag was provided

  -help: print this usage
  -version: print current script's version
  -sensorVersion <VersionInfo>: select sensor's version; e.g.: '-sensorVersion 3.4.1.0.win64';
 will download the latest version by default if this flag was not provided
  -ls: list all available sensor versions for your system (will not list pre-3.1 packages);
 will not download any package
  -file <FileName>: provide local zip file to install sensor instead of downloading it from
 cluster
  -save <FileName>: downloaded and save zip file as <FileName>
  -new: remove any previous installed sensor; previous sensor identity has to be removed
from cluster in order for the new registration to succeed
  -reinstall: reinstall sensor and retain the same identity with cluster; this flag has
higher priority than -new
  -npcap: overwrite existing npcap
  -forceUpgrade: force sensor upgrade to version given by -sensorVersion flag; e.g.:
'-sensorVersion 3.4.1.0.win64 -forceUpgrade'; apply the latest version by default if
-sensorVersion flag was not provided
  -upgradeLocal: trigger local sensor upgrade to version given by -sensorVersion flag; e.g.:
 '-sensorVersion 3.4.1.0.win64 -upgradeLocal'; apply the latest version by default if
-sensorVersion flag was not provided
```

```
  -upgradeByUUID <FileName>: trigger sensor whose uuid is listed in <FileName> upgrade to
version given by -sensorVersion flag; e.g.: '-sensorVersion 3.4.1.0.win64 -upgradeByUUID
"C:\\Program Files\\Cisco Tetration\\sensor_id"'; apply the latest version by default if
-sensorVersion flag was not provided
  -visibility: install deep visibility agent only; -reinstall would overwrite this flag if
 previous installed agent type was enforcer
  -goldenImage: install Cisco Secure Workload Agent but do not start the Cisco Secure
Workload Services; use to install Cisco Secure Workload Agent on Golden Images in VDI
environment or Template VM. On VDI/VM instance created from golden image with different
host name, Cisco Secure Workload Services will work normally
  -installFolder: install Cisco Secure Workload Agent in a custom folder specified by
-installFolder e.g.: '-installFolder "c:\\custom sensor path"'; default path is "C:\Program
 Files\Cisco Tetration"
```

Installer l'agent Windows à l'aide de la méthode du programme d'installation de l'image de l'agent

Nous vous recommandons d'utiliser la méthode du script d'installation automatisé pour installer les agents Windows. Utilisez la méthode de l'installation par image si vous avez une raison précise d'utiliser cette méthode manuelle.

Note Ne déployez pas manuellement une version antérieure de l'agent MSI lorsqu'un agent existant est déjà en cours d'exécution sur l'hôte.

Les fichiers liés au site qui se trouvent dans le paquet :

- **ca.cert** - Obligatoire : certificat de l'autorité de certification pour les communications des capteurs.
- **enforcer.cfg** - Obligatoire uniquement lors de l'installation du capteur d'application - Contient la configuration des points terminaux de mise en application.
- **sensor_config** - Obligatoire : configuration pour le capteur de visibilité approfondie.
- **sensor_type :**Type de capteur (mise en application ou visibilité approfondie).
- **site.cfg** : obligatoire : configuration du point terminal de site global.
- **user.cfg :**obligatoire pour les logiciels-services : configuration de la clé d'activation du capteur et du serveur mandataire.

Prérequis

Configurez ACTIVATION_Key et HTTPS_PROXY dans le fichier user.cfg pour les grappes de logiciels-services et lorsque vous installez l'agent sur un détenteur autre que par défaut, des grappes sur site à plusieurs détenteurs. Pour en savoir plus, consultez (installations manuelles seulement) Mettre à jour le fichier de configuration utilisateur.

Pour installer un agent Windows à l'aide de la méthode de l'image de l'agent :

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).

- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Image Installer** (Programme d'installation de l'image de l'agent).

Étape 3 Dans le champ **Platform** (plateforme), saisissez Windows.

Étape 4 Saisissez le type et la version de l'agent requis, puis, à partir des résultats, téléchargez la version de l'agent nécessaire.

Étape 5 Copier le fichier *tet-win-sensor*<*version*>.*win64-*<*clustername*>.*zip*sur tous les hôtes Windows pour le déploiement.

Étape 6 Assurez-vous que vous disposez de privilèges d'administration et extrayez le fichier ZIP.

Étape 7 Dans le dossier extrait, exécutez la commande suivante pour installer l'agent : `msiexec.exe /i TetrationAgentInstaller.msi`

En outre, les options suivantes sont disponibles pour le programme d'installation MSI.

Table 2: Options disponibles pour le programme d'installation MSI

Options	Description
agenttype=<AgentType>	*AgentType* doit être soit *capteur* ou *appliqueur*, selon que l mise en application est requise ou non. Par défaut, le programme d'installation vérifie le contenu du fichier sensor_type dans le même dossier et utilise le contenu pour remplacer le paramètre transmis. Toutefois, si l'agent est installé en mode */quiet*, l'option est obligatoire.
overwritenpcap=yes	Pour Windows 2008 R2, par défaut, l'agent ne tente pas de mettre à niveau Npcap si Npcap existe déjà. Transmettez ce paramètre pour mettre à niveau le Npcap existant. Si cette option est utilisée, les mises à niveau automatiques suivantes des agents mettent également à niveau de Npcap vers les versions les plus récentes prises en charge.
nostart=yes	Transmettez ce paramètre, lors de l'installation de l'agent à l'aide d'une image idéale dans un environnement VDI ou un modèle de machine virtuelle, pour empêcher le service d'agent TetSensor TetEnforcer CswAgent de démarrer automatiquement. Sur les instances de VDI/VM créées à l'aide de l'image idéale et avec un nom d'hôte différent, ces services, comme prévu, démarrent automatiquement.
installfolder=<FullPathCustomFolder>	Utilisez ce paramètre, à la fin de la commande install, pour installer l'agent dans un dossier personnalisé.

Options	Description
serviceuser=<Service UserName>	Utilisez ce paramètre, à la fin de la commande install, pour configurer l'utilisateur du service. L'utilisateur du service par défaut est « LocalSystem ». Pour l'utilisateur local, serviceuser=.\<Service UserName> Pour l'utilisateur de domaine, serviceuser=<domain_name>\<samaccount name> L'utilisateur de service doit disposer de privilèges d'administration locale.
servicepassword=<Service UserPassword>	Utilisez ce paramètre, à la fin de la commande install, pour configurer le mot de passe de l'utilisateur du service. Le mot de passe doit être en format de texte brut.
proxy="<proxy_address>"	Utilisez ce paramètre pour définir le serveur mandataire HTTPS pour accéder à la grappe Cisco Secure Workload.
activationkey=<activation Key>	Utilisez ce paramètre pour préciser le détenteur si l'agent n'est pas installé sous le détenteur par défaut.

Note

- Si la clé d'activation et les options de serveur mandataire sont utilisées pendant l'installation manuelle, vous n'avez pas besoin de configurer manuellement le fichier *user.cfg*.
- Pour les systèmes d'exploitation Windows autres que Windows 2008 R2, lorsque vous mettez à niveau à la version 3.8, le Npcap installé est automatiquement désinstallé par l'agent Windows.
- Si l'agent est déjà installé sur l'hôte, ne le réinstallez pas. Pour mettre à niveau l'agent, consultez la section Mise à niveau des agents logiciels.

Vérifier l'installation de l'agent Windows

Procedure

Étape 1 Vérifiez que le dossier `C:\\Program Files\\Cisco Tetration` (ou le dossier personnalisé) existe.

Étape 2 Vérifiez que le service*TetSensor CswAgent*, pour une visibilité et une application approfondies, existe et qu'il est en cours d'exécution. Exécutez la commande `cmd.exe` avec des privilèges d'administration.

Exécutez la commande `sc query tetsensor sc query cswagent`

Vérifiez si l'état est **Running** (En cours d'exécution)

Exécuter la commande `sc qc tetsensorsc qc cswagent`

Vérifiez si DISPLAY-NAME est **Cisco Secure Workload Deep Visibility** (Visibilité approfondie de Cisco Secure Workload)

OU

Exécutez la commande **services.msc**

Trouvez le nom de **Cisco Secure Workload Deep Visibility** (Visibilité approfondie de Cisco Secure Workload)

Vérifiez si l'état est **Running** (En cours d'exécution)

Vérification de l'agent Windows dans le contexte utilisateur du service configuré

1. Vérifiez que les protocoles TetSensor (pour la visibilité approfondie) et TetEnforcer (pour la mise en application) s'exécutent dans le contexte d'utilisateur de service configuré. TetSensor et TetEnforcer s'exécutent dans le même contexte d'utilisateur de service.

   Assurez-vous que le service CswAgent en cours d'exécution dans le contexte d'utilisateur de service configuré. CswAgent s'exécute dans le même contexte d'utilisateur de service.

   Exécutez la commande `cmd.exe` avec des privilèges d'**administrateur**.

   Exécuter la commande `sc qc tetsensorsc qc cswagent`

   Cochez SERVICE_START_NAME.<utilisateur du service configuré>

   Exécutez la commande `sc qc tetenforcer`

   Cochez SERVICE_START_NAME.<utilisateur du service configuré>

   OU

   Exécutez la commande `services.msc`

   Trouvez le nom de **Cisco Secure Workload Deep Visibility** (Visibilité approfondie de Cisco Secure Workload)

   Cochez **Log On As (Ouvrir une session en tant que)** pour l'<utilisateur du service configuré>

   Trouvez le nom **Cisco Secure Workload Enforcement.**

   Cochez **Log On As (Ouvrir une session en tant que)** pour l'<utilisateur du service configuré>

   OU

   Exécutez la commande `tasklist /v | find /i "tet"`

   Exécutez la commande `tasklist /v | find /i "cswengine"`

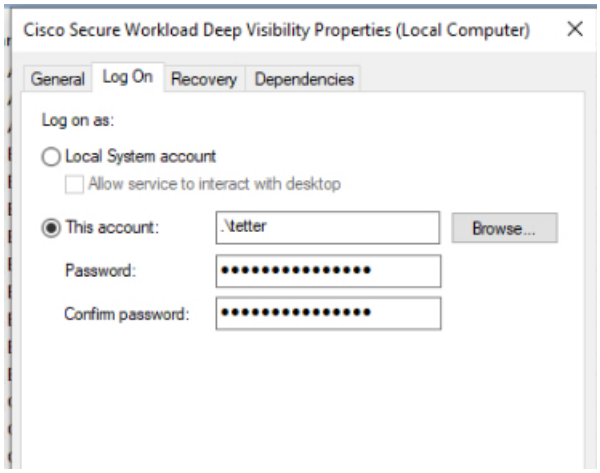
   Vérifier le contexte utilisateur pour les processus en cours d'exécution (5e colonne)

Modifier le compte de service

Après avoir installé les agents Windows, utilisez l'une des méthodes suivantes pour modifier les services de visibilité approfondie et de mise en application existants.

- Utilisez **services.msc**.

Illustration 9 : Modifier le compte de service en fonction du compte services.msc



- Utilisez une application tierce pour configurer les services.
- Utilisez les commandes suivantes :

1. Exécutez cmd en tant qu'administrateur.
2. Modifiez les services à l'aide du nom du compte de service en exécutant les commandes suivantes :
   1. `sc config tetsensor obj= <service user name> password= <password>`
   2. `sc config tetenforcer obj= <service user name> password= <password>`
      - sc config cswagent obj= <service user name> password= <password>
3. Vérifiez les configurations de service en exécutant les commandes suivantes :
   1. `sc qc tetsensor`
   2. `sc qc tetenforcer`
      - `sc qc cswagent`
4. Redémarrez les services tetsensor et tetenforcer en exécutant les commandes suivantes :

   Redémarrez le service CswAgent en exécutant les commandes suivantes :

   1. `sc stop tetsensor / tetenforcer`
   2. `sc start tetsensor / tetenforcer`

   1. sc stop cswagent
   2. sc start cswagent

Déploiement des agents sur une instance VDI ou un modèle de machine virtuelle (Windows)

Par défaut, les services d'agent démarrent automatiquement après l'installation des agents. Lors de l'installation sur une image idéale (golden), vous devez utiliser des indicateurs d'installation pour empêcher ces services de démarrer. Lorsque des instances sont dupliquées à partir de l'image idéale, les services d'agent, comme prévu, démarrent automatiquement.

L'agent n'installera pas NPCAP sur les machines virtuelles golden, mais sera automatiquement installé si nécessaire sur les instances de VM clonées à partir d'une image golden. Pour en savoir plus, consultez Programme d'installation de l'agent Windows et Npcap : pour Windows 2008 R2.

Installer l'agent sur une image idéale dans un environnement VDI ou un modèle de machine virtuelle

Procedure

Étape 1 Installez l'agent sur une image idéale dans un environnement VDI ou un modèle de machine virtuelle à l'aide d'un programme d'installation MSI ou d'un script d'installation PowerShell :

Utiliser le programme d'installation MSI avec **nostart=yes**

- Pour en savoir plus, consultez Installer l'agent Windows à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 30.
- msiexec.exe /<MSI installer> nostart="yes" /quiet /norestart /l*v <installer_log_file> OU

OU

Utilisez le programme d'installation PowerShell avec l'indicateur **-goldenImage**.

- Pour en savoir plus, consultez Installer l'agent Windows à l'aide de la méthode du programme d'installation du script de l'agent, on page 28.

Étape 2 Vérifiez que le dossier `C:\\Program Files\\Cisco Tetration` (ou le dossier personnalisé) existe.

Étape 3 Assurez-vous que le service TetSensor (pour une visibilité approfondie) existe et qu'il est arrêté :

Exécutez la commande `cmd.exe` avec des privilèges d' **administrateur**.

Exécutez la commande `sc query tetsensor`.

Vérifiez si STATE (ÉTAT) est **arrêté**.

Étape 4 Assurez-vous que le service TetEnforcer (pour la mise en application) existe et qu'il est arrêté :

Exécutez la commande **sc query tetenforcer**.

Vérifiez si STATE (ÉTAT) est arrêté.

.

Étape 5 Vérifiez que le service CswAgent existe et qu'il est arrêté :

Exécutez la commande `cmd.exe` avec des privilèges d' **administrateur**.

Exécutez la commande `sc query cswagent`

Vérifiez si STATE (ÉTAT) est **arrêté**.

Étape 6 Le modèle de machine virtuelle est maintenant configuré.

Étape 7 Arrêtez le modèle de machine virtuelle.

Créer une nouvelle instance de machine virtuelle VDI

Procedure

Étape 1 Créez une nouvelle machine virtuelle d'instance VDI en dupliquant le modèle de machine virtuelle.

Étape 2 Redémarrez la machine virtuelle de l'instance VDI.

Étape 3 Après avoir redémarré la machine virtuelle de l'instance VDI, assurez-vous que les services – TetSensor (pour une visibilité approfondie) et TetEnforcer (pour l'application) – s'exécutent dans le contexte de service configuré. Reportez-vous à la section Vérifier l'installation de l'agent Windows.

Étape 4 Après avoir redémarré la machine virtuelle de l'instance VDI, vérifiez que le service CswAgent est en cours d'exécution dans le contexte de service configuré. Reportez-vous à la section Vérifier l'installation de l'agent Windows.

Étape 5 Sur la machine virtuelle de l'instance VDI, assurez-vous que le pilote NPCAP est installé et en cours d'exécution :

Exécutez la commande `cmd.exe` avec des privilèges d'administrateur.

Exécutez la commande `sc query npcap`

Vérifiez si STATE (ÉTAT) est égal à **Running** (Exécution en cours)

Étape 6 Sur la machine virtuelle de l'instance VDI, assurez-vous que l'agent est enregistré à l'aide d'un sensor_id (identifiant de capteur) valide :

- Vérifiez le fichier Sensor_id dans le dossier d'installation.
- Si sensor_id commence par « uuid », il ne s'agit pas d'un sensor_id valide.
- Si l'agent ne s'enregistre pas, mais que l'interface Web Cisco Secure Workload indique que l'agent est enregistré :
- Supprimez l'agent à l'aide d'OpenAPI. Pour en savoir plus, consultez la section Déployer des agents logiciels.

Note

- Ne modifiez pas le nom d'hôte de l'image golden (idéale) ou du modèle de machine virtuelle.
- Si l'image idéale ou le modèle de machine virtuelle est redémarré après l'installation de l'agent, les services Cisco Secure Workload commencent à s'exécuter après le redémarrage.
- Si la machine virtuelle de l'instance VDI ne signale pas les flux de réseau, consultez la section *Machine virtuelle de l'instance VDI dans les flux réseau*.

.

Programme d'installation de l'agent Windows et Npcap : pour Windows 2008 R2

1. Pour les versions de Npcap prises en charge, consultez la matrice de prise en charge à l'adresse https://www.cisco.com/go/secure-workload/requirements/agents.

2. Installation :

   Si Npcap n'est pas installé, l'agent installe la version prise en charge dix secondes après le démarrage du service. Si Npcap est installé chez l'utilisateur, mais que la version est antérieure à la version prise en charge, Npcap n'est pas mis à niveau. Mettez à niveau ou désinstallez manuellement Npcap, exécutez le programme d'installation de l'agent en incluant l'option **overwritenpcap=yes** ou exécutez le script d'installation avec **-npcap** pour obtenir la version de Npcap prise en charge. Si le pilote Npcap est en cours d'utilisation par une application, l'agent met à niveau Npcap ultérieurement.

3. Mettre à niveau :

   Si Npcap est installé par l'agent Windows et que la version est antérieure à la version prise en charge, Npcap est mis à niveau à la version prise en charge dix secondes après le démarrage du service. Si le pilote Npcap est en cours d'utilisation par une application, l'agent met à niveau Npcap ultérieurement. Si Npcap n'est pas installé par l'agent Windows, Npcap n'est pas mis à niveau.

4. Désinstaller :

   Si Npcap est installé par l'agent Windows, l'agent désinstalle Npcap. Si Npcap est installé par l'utilisateur, mais mis à niveau par le programme d'installation de l'agent avec l'option **overwritenpcap=yes**, Npcap n'est pas désinstallé. Si le pilote Npcap est utilisé par une application, l'agent ne désinstalle pas Npcap.

Captures de flux de l'agent Windows : pour tous les systèmes d'exploitation Windows, à l'exception de Windows Server 2008 R2

À partir de la dernière version de Windows, l'agent utilise le pilote ndiscap.sys (intégré à Microsoft) et le cadre Events Tracing using Windows (ETW) pour capturer les flux du réseau.

Lors de la mise à jour vers la dernière version :

- L'agent passe à ndiscap.sys à partir de npcap.sys.
- Le programme d'installation de l'agent désinstalle Npcap si :
  - Npcap est installé par l'agent.
  - Npcap n'est pas utilisé.
  - La version du système d'exploitation n'est pas Windows Server 2008 R2.

Une fois les services de l'agent démarrés, l'agent crée des sessions ETW, CSW_MonNet et CSW_MonDns (pour les données DNS), et lance la capture des flux réseau.

Note

- Sur Windows Server 2012, les paquets réseau sont analysés pour trouver les données DNS.
- L'agent Windows sur les hôtes sous Windows Server 2012 et versions ultérieures capture les noms d'utilisateur du consommateur et du fournisseur et les noms d'utilisateur sont disponibles dans les observations de flux. Cette fonctionnalité n'est pas prise en charge sur Windows Server 2008 R2 en raison des limites du système d'exploitation. Dans le profil de configuration de l'agent, configurez les éléments suivants pour capturer les noms d'utilisateur :
  - Activer la recherche de PID/utilisateur
  - Réglez Flow Analysis Fidelity (fidélité de l'analyse de flux) à Detailed (détaillé).

Installation des agents AIX pour une visibilité approfondie et une mise en application

Note Les fonctions d'arborescence de processus, de paquet (CVE) et de rapports sur les événements criminalistiques ne sont pas disponibles sur AIX. En outre, certains aspects de ces fonctionnalités peuvent ne pas être disponibles dans des versions mineures spécifiques de plateformes prises en charge en raison des limites du système d'exploitation.

Configuration requise et conditions préalables à l'installation des agents AIX

- Consultez la section Supported Platforms and Requirements.
- Exigences supplémentaires pour une visibilité approfondie :
  - Privilèges racine pour installer et exécuter les services.
  - Exigences de stockage pour les fichiers d'agent et de journaux : 500 Mo.
  - Les exclusions de sécurité configurées sur toutes les applications de sécurité qui surveillent l'hôte. Ces exclusions visent à empêcher d'autres applications de sécurité de bloquer l'installation ou l'activité des agents. Pour en savoir plus, consultez Exclusions de sécurité.
  - AIX prend en charge la capture de flux de seulement 20 périphériques réseau (6 périphériques réseau si la version est AIX 7.1 TL3 SP4 ou antérieure). L'agent de visibilité approfondie effectue la capture à partir d'un maximum de 16 périphériques réseau, laissant les quatre autres sessions de capture disponibles pour une utilisation générique exclusive du système (par exemple, tcpdump).
  - L'agent de visibilité en profondeur effectue les opérations suivantes pour assurer la capture des flux de 20 périphériques réseau :
    - L'agent crée 16 nœuds de périphérique bpf dans le répertoire agents (/opt/cisco/tetration/chroot/dev/bpf0 à /opt/cisco/tetration/chroot/dev/bpf15)
    - tcpdump et d'autres outils système utilisant bpf analyseront les nœuds du périphérique système (/dev/bpf0 à /dev/bpf19) jusqu'à ce qu'ils trouvent un nœud inutilisé (!EBUSY).
    - Les nœuds bpf créés par l'agent et les nœuds bpf du système partagent les mêmes majeures/mineures, chaque majeure ou mineure étant ouverte par une seule instance (tcpdump ou agent).
    - L'agent n'accède pas aux nœuds du périphérique système et ne les crée pas comme le fait tcpdump (tcpdump-D crée /dev/bpf0. . . /dev/bpf19 s'ils n'existent pas).
  - L'exécution d'iptrace sur le système empêche, dans certains scénarios, la capture du flux à partir de tcpdump et de l'agent de visibilité approfondie. Il s'agit d'un problème de conception connu qui doit être vérifié auprès d'IBM.
    - Pour vérifier si ce scénario existe, avant d'installer l'agent, exécutez tcpdump. Si le message d'erreur est **tcpdump: BIOCSETIF: en0: File exists** iptrace bloque la capture de flux. Arrêtez iptrace pour résoudre le problème.

- Toutes les fonctions de visibilité approfondie ne sont pas prises en charge dans AIX. La comptabilité des paquets et des processus fait partie de celles qui ne sont pas prises en charge.

- Exigences supplémentaires pour l'application des politiques :
  - Si le filtre de sécurité IP est activé (c'est-à-dire, smitty IPsec4), l'installation de l'agent échoue lors de la vérification préalable. Nous vous recommandons de désactiver le filtre de sécurité IP avant d'installer l'agent.
  - Si la sécurité IP est activée lorsque l'agent de mise en application de Cisco Secure Workload est en cours d'exécution, une erreur est signalée et l'agent d'application arrête l'application de la politique. Communiquez avec le service d'assistance pour désactiver en toute sécurité le filtre de sécurité IP lorsque l'agent de mise en application est en cours d'exécution.

Installer l'agent AIX à l'aide de la méthode du programme d'installation du script de l'agent

Les agents AIX de visibilité et d'application en profondeur ne peuvent être installés qu'à l'aide de la méthode d'installation par script de l'agent.

Note
- L'agent AIX installé prend en charge la visibilité approfondie et l'application.
- Le paramètre par défaut est Disabled (désactivé). Pour activer l'application, consultez Creating an Agent Config Profile, on page 83.

Pour installer un agent AIX :

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :
- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Script Installer** (Installateur de script d'agent).

Étape 3 Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez **AIX**.

Pour afficher les plateformes AIX prises en charge, cliquez sur **Show Supported Platforms** (Afficher les plateformes prises en charge).

Étape 4 Choisissez le détenteur pour installer les agents.

Note La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.

Étape 5 Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.

Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont automatiquement attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :

- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
- Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.

Étape 6 Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.

Étape 7 Dans la section **Installer expiration** (Expiration de la validité de l'installateur), sélectionnez une option parmi celles disponibles :

- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
- Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
- Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
- Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.

Étape 8 Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

Étape 9 Copiez le script Shell du programme d'installation sur tous les hôtes AIX pour le déploiement.

Étape 10 Pour accorder l'autorisation d'exécution au script, exécutez la commande : `chmod u+x tetration_installer_default_sensor_aix.sh`

Note Le nom du script peut différer selon le type et la portée de l'agent.

Étape 11 Pour installer l'agent, exécutez la commande suivante avec les privilèges racine : `./tetration_installer_default_sensor_aix.sh`

Note Si un agent est déjà installé sur l'hôte, vous ne pouvez pas poursuivre l'installation.

Nous vous recommandons d'exécuter la vérification préalable, comme spécifié dans les détails d'utilisation du script.

Détails de l'utilisation du script d'installation d'AIX :

```
ksh tetration_installer_default_enforcer_aix.sh [--pre-check] [--pre-check-user]
[--skip-pre-check=<option>] [--no-install] [--logfile=<filename>] [--proxy=<proxy_string>]
 [--no-proxy] [--help] [--version] [--sensor-version=<version_info>] [--ls]
[--file=<filename>] [--osversion=<osversion>] [--save=<filename>] [--new] [--reinstall]
[--unpriv-user] [--libs=<libs.zip|tar.Z>] [--force-upgrade] [--upgrade-local]
[--upgrade-by-uuid=<filename>] [--logbasedir=<logbdir>] [--tmpdir=<tmp_dir>] [--visibility]
 [--golden-image]
  --pre-check: run pre-check only
  --pre-check-user: provide alternative to nobody user for pre-check su support
  --skip-pre-check=<option>: skip pre-installation check by given option; Valid options
include 'all', 'ipv6' and 'enforcement'; e.g.: '--skip-pre-check=all' will skip all
pre-installation checks; All pre-checks will be performed by default
  --no-install: will not download and install sensor package onto the system
  --logfile=<filename>: write the log to the file specified by <filename>
```

```
  --proxy=<proxy_string>: set the value of HTTPS_PROXY, the string should be formatted as
http://<proxy>:<port>
  --no-proxy: bypass system wide proxy; this flag will be ignored if --proxy flag was
provided
  --help: print this usage
  --version: print current script's version
  --sensor-version=<version_info>: select sensor's version; e.g.: '--sensor-version=3.4.1.0';
 will download the latest version by default if this flag was not provided
  --ls: list all available sensor versions for your system (will not list pre-3.3 packages);
 will not download any package
  --file=<filename>: provide local zip file to install sensor instead of downloading it
from cluster
  --osversion=<osversion>: specify osversion for --save flag;
  --save=<filename>: download and save zip file as <filename>; will download package for
osversion given by --osversion flag; e.g.: '--save=myimage.aix72.tar.Z --osversion=7.2'
  --new: remove any previous installed sensor; previous sensor identity has to be removed
from cluster in order for the new registration to succeed
  --reinstall: reinstall sensor and retain the same identity with cluster; this flag has
higher priority than --new
  --unpriv-user=<username>: use <username> for unpriv processes instead of tet-snsr
  --libs=<libs.zip|tar.Z>: install provided libs to be used by agents
  --force-upgrade: force sensor upgrade to version given by --sensor-version flag; e.g.:
'--sensor-version=3.4.1.0 --force-upgrade'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-local: trigger local sensor upgrade to version given by --sensor-version flag:
 e.g.: '--sensor-version=3.4.1.0 --upgrade-local'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-by-uuid=<filename>: trigger sensor whose uuid is listed in <filename> upgrade
to version given by --sensor-version flag; e.g.: '--sensor-version=3.4.1.0
--upgrade-by-uuid=/usr/local/tet/sensor_id'; apply the latest version by default if
--sensor-version flag was not provided
  --logbasedir=<log_base_dir>: instead of logging to /opt/cisco/tetration/log use
<log_base_dir>. The full path will be <log_base_dir>/tetration
  --tmpdir=<tmp_dir>: instead of using /tmp use <tmp_dir> as temp directory
  --visibility: install deep visibility agent only; --reinstall would overwrite this flag
if previous installed agent type was enforcer
  --golden-image: install Cisco Secure Workload Agent but do not start the Cisco Secure
Workload Services; use to install Cisco Secure Workload Agent on Golden Images in VDI
environment or Template VM. On VDI/VM instance created from golden image with different
host name, Cisco Secure Workload Services will work normally
```

Vérifier l'installation de l'agent AIX

Procédure

Exécutez la commande `lslpp -c -l tet-sensor.rte`, confirmez qu'il y a une entrée comme suit.

Remarque La sortie spécifique peut différer selon la version

`$ sudo lslpp -c -l tet-sensor.rte` /usr/lib/objrepos:tet-sensor.rte:3.4.1.19::COMMITTED:I:TET tet sensor package:

```
$ sudo lssrc -s tet-sensor
```

État PID de groupe de sous-systèmes tet-sensor 1234567 active

```
$ sudo lssrc -s tet-enforcer
```

État PID de groupe de sous-systèmes tet-enforcer 7654321 actif

Installer les agents Kubernetes ou OpenShift pour une visibilité et une application approfondies

Requirements and Prerequisites

Kubernetes 1.[16-22]

- RHEL: 7.[0-9] (only x86_64 architecture)
- CentOS: 7.[0-8] (only x86_64 architecture)
- Oracle Linux: 7.[0-8] (only x86_64 architecture)
- Ubuntu: 16.04, 18.04, 20.04 (only x86_64 architecture)
- SUSE Linux Enterprise Server: 12sp[0-5] (only x86_64 architecture)
- Amazon Linux 2 (only x86_64 architecture)

Openshift 4.[5-9]

- Red Hat Enterprise Linux CoreOS: 4.[5-9] (only x86_64 architecture)

Container Runtime

- Docker
- CRI-O
- containerd (>= 1.5.x)

Note For containerd runtime, if the config_path is not set, modify your config.toml (default location: /etc/containerd/config.toml) as follows:

[plugins.”io.containerd.grpc.v1.cri”.registry] config_path = “/etc/containerd/certs.d”

Restart the containerd daemon.

Additional Requirements

- The install script requires Kubernetes or OpenShift admin credentials to start privileged agent pods on the cluster nodes.
- Secure Workload entities are created in a namespace named ‘tetration’.
- The node or pod security policies should permit privileged mode pods.

- busybox:1.33 images should either be pre-installated or downloadable from Docker Hub.
- In order to run on Kubernetes or OpenShift control plane nodes, the *–toleration* flag can be used to pass in a toleration for the Cisco Secure Workload pods. This usually is the NoSchedule toleration that normally prevents pods from running on control plane nodes.

Requirements for Policy Enforcement

Agents enforcing policy on container orchestration platforms are supported on RHEL 7.[0-9], CentOS 7.[0-8] or Ubuntu 16.04/18.04/20.04 nodes.

IPVS based kube-proxy mode is not supported for OpenShift.

These agents should be configured with the Preserve Rules option enabled. See Creating an Agent Config Profile.

For enforcement to function properly, any installed CNI plugin must:

- Provide a flat address space (IP network) between all nodes and pods. Network plugins which masquerade the source pod IP for intra-cluster communication are not supported.
- Not interfere with Linux iptables rules or marks used by the Cisco Secure Workload Enforcement Agent (mark bits 21 and 20 are used to allow and deny traffic for NodePort services)

The following CNI plugins have been tested to meet the requirements above:

- Calico (3.13) with the following Felix configurations: *(ChainInsertMode: Append, IptablesRefreshInterval: 0)* or *(ChainInsertMode: Insert, IptablesFilterAllowAction: Return, IptablesMangleAllowAction: Return, IptablesRefreshInterval: 0)*. All other options use their default values.

See the Felix configuration reference for more information on setting these options.

Installer l'agent Kubernetes ou OpenShift à l'aide de la méthode du programme d'installation du script de l'agent

Note La méthode du programme d'installation du script de l'agent installe automatiquement les agents sur les nœuds inclus ultérieurement.

Procedure

Étape 1 Accédez aux méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Script Installer** (Installateur de script d'agent).

Étape 3 Dans le menu déroulant **Select Platform** (Sélectionner une plateforme), choisissez **Kubernetes**.

Pour afficher les plateformes Kubernetes ou OpenShift prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).

Étape 4 Choisissez le détenteur pour installer les agents.

Note La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.

Étape 5 Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.

Étape 6 Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

Étape 7 Exécutez le script d'installation sur une machine Linux qui a accès au serveur d'API Kubernetes et à un fichier de configuration kubectl avec des privilèges d'administration comme contexte/grappe/utilisateur par défaut.

Le programme d'installation tente de lire le fichier à partir de son emplacement par défaut (~/.kube/config). Cependant, vous pouvez spécifier explicitement l'emplacement du fichier de configuration à l'aide de la commande --kubeconfig.

Le script d'installation fournit des instructions sur la vérification du daemonset de l'agent Cisco Secure Workload et des pods installés.

Note Le serveur mandataire HTTP configuré sur la page du programme d'installation de l'agent avant le téléchargement contrôle uniquement la façon dont les agents Cisco Secure Workload se connectent à la grappe Cisco Secure Workload. Ce paramètre n'affecte pas la façon dont les images Docker sont extraites par les nœuds Kubernetes ou OpenShift, car l'environnement d'exécution du conteneur sur ces nœuds utilise sa propre configuration de serveur mandataire. Si les images Docker ne sont pas extraites de la grappe Cisco Secure Workload, déboguer le processus d'extraction d'image du conteneur et ajouter un serveur mandataire HTTP approprié.

Installation des agents Solaris pour une visibilité approfondie

Configuration requise et conditions préalables à l'installation des agents Solaris

- Consultez la section Supported Platforms and Requirements.
- Privilèges racine pour installer et exécuter les services.
- Un Go d'espace de stockage pour les fichiers des agents et des journaux.
- Configuration des exclusions de sécurité sur les applications de sécurité qui surveillent l'hôte, afin d'empêcher d'autres applications de sécurité de bloquer l'installation ou l'activité de l'agent. Pour en savoir plus, consultez Exclusions de sécurité.

Installer l'agent Solaris à l'aide de la méthode du programme d'installation du script de l'agent

L'agent Solaris installé prend en charge à la fois la visibilité en profondeur et la visibilité des processus ou des paquets.

Procedure

Étape 1 Accédez à Méthodes d'installation des agents :

- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
- Dans le volet de navigation, choisissez **Manage** > **Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).

Étape 2 Cliquez sur **Agent Script Installer** (Installateur de script d'agent).

Étape 3 Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez « **Solaris »**.

Pour afficher les plateformes Solaris prises en charge, cliquez sur **Show Supported Platforms**(Afficher les plateformes prises en charge).

Étape 4 Choisissez le détenteur pour installer les agents.

Note La sélection du détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.

Étape 5 Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.

Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont automatiquement attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :

- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
- Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.

Étape 6 Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.

Étape 7 Dans la section **Installer expiration** (Expiration de la validité de l'installateur), sélectionnez une option parmi celles disponibles :

- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
- Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
- Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
- Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.

Étape 8 Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

Étape 9 Copiez le script du shell d'installation sur les hôtes Solaris et exécutez la commande suivante pour accorder l'autorisation d'exécution au script : `chmod u+x tetration_installer_default_sensor_solaris.sh`

Note Le nom du script peut différer selon le type d'agent et la portée sélectionnés.

Étape 10 Pour installer l'agent, exécutez la commande suivante avec les privilèges d'utilisateur racine : `./tetration_installer_default_sensor_solaris.sh`

Note Si un agent est déjà installé sur le détenteur, vous ne pouvez pas poursuivre l'installation.

Nous vous recommandons d'exécuter la vérification préalable, comme spécifié dans les détails d'utilisation du script.

Détails d'utilisation du script d'installation de Cisco Solaris :

```
tetration_installer_default_sensor_solaris.sh [--pre-check] [--skip-pre-check=<option>]
[--no-install] [--logfile=<filename>] [--proxy=<proxy_string>] [--no-proxy] [--help]
[--version] [--sensor-version=<version_info>] [--ls] [--file=<filename>] [--save=<filename>]
 [--new] [--reinstall] [--unpriv-user] [--force-upgrade] [--upgrade-local]
[--upgrade-by-uuid=<filename>] [--basedir=<basedir>] [--logbasedir=<logbdir>]
[--tmpdir=<tmp_dir>] [--visibility] [--golden-image]
  --pre-check: run pre-check only
  --skip-pre-check=<option>: skip pre-installation check by given option; Valid options
include 'all', 'ipv6' and 'enforcement'; e.g.: '--skip-pre-check=all' will skip all
pre-installation checks; All pre-checks will be performed by default
  --no-install: will not download and install sensor package onto the system
  --logfile=<filename>: write the log to the file specified by <filename>
  --proxy=<proxy_string>: set the value of CL_HTTPS_PROXY, the string should be formatted
as http://<proxy>:<port>
  --no-proxy: bypass system wide proxy; this flag will be ignored if --proxy flag was
provided
  --help: print this usage
  --version: print current script's version
  --sensor-version=<version_info>: select sensor's version; e.g.: '--sensor-version=3.4.1.0';
 will download the latest version by default if this flag was not provided
  --ls: list all available sensor versions for your system (will not list pre-3.1 packages);
 will not download any package
  --file=<filename>: provide local zip file to install sensor instead of downloading it
from cluster
  --save=<filename>: download and save zip file as <filename>
  --new: remove any previous installed sensor; previous sensor identity has to be removed
from cluster in order for the new registration to succeed
  --reinstall: reinstall sensor and retain the same identity with cluster; this flag has
higher priority than --new
  --unpriv-user=<username>: use <username> for unpriv processes instead of nobody
  --force-upgrade: force sensor upgrade to version given by --sensor-version flag; e.g.:
'--sensor-version=3.4.1.0 --force-upgrade'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-local: trigger local sensor upgrade to version given by --sensor-version flag:
 e.g.: '--sensor-version=3.4.1.0 --upgrade-local'; apply the latest version by default if
--sensor-version flag was not provided
  --upgrade-by-uuid=<filename>: trigger sensor whose uuid is listed in <filename> upgrade
to version given by --sensor-version flag; e.g.: '--sensor-version=3.4.1.0
--upgrade-by-uuid=/usr/local/tet/sensor_id'; apply the latest version by default if
--sensor-version flag was not provided
  --logbasedir=<log_base_dir>: instead of logging to /opt/cisco/secure-workload/log use
<log_base_dir>. The full path will be <log_base_dir>/secure-workload
  --tmpdir=<tmp_dir>: instead of using /tmp use <tmp_dir> as temp directory
  --visibility: install deep visibility agent only; --reinstall would overwrite this flag
if previous installed agent type was enforcer
```

```
  --golden-image: install Cisco Secure Workload Agent but do not start the Cisco Secure
Workload Services; use to install Cisco Secure Workload Agent on Golden Images in VDI
environment or Template VM. On VDI/VM instance created from golden image with different
host name, Cisco Secure Workload Services will work normally
```

Vérifier l'installation de l'agent Solaris

Procedure

Étape 1 Exécutez la commande : `sudo pkg list tet-sensor`

Étape 2 Une seule entrée constituant la sortie confirme qu'un agent Solaris est installé sur l'hôte.
Exemple de sortie :

NAME (PUBLISHER)	VERSION	IFO
tet-capteur (cisco)	3.8.1.1	i--

Note La sortie spécifique peut différer en fonction de la plateforme et de l'architecture.

(installations manuelles seulement) Mettre à jour le fichier de configuration utilisateur

La procédure suivante est requise uniquement pour les installations impliquant *tous* les éléments suivants :

- Le logiciel-service ou grappes sur site Cisco Secure Workload avec plusieurs détenteurs (les grappes sur site qui utilisent uniquement le détenteur par défaut n'ont PAS besoin de cette procédure)
- Installation manuelle
- Plateforme Linux ou Windows

Les agents ont besoin d'une clé d'activation pour s'enregistrer sur la grappe Cisco Secure Workload. ils nécessitent une clé d'activation de grappe. En outre, ils peuvent avoir besoin d'un serveur mandataire HTTPS pour atteindre la grappe.

Note Dans un environnement Windows, vous n'avez pas besoin de configurer manuellement le fichier user.cfg, si les options de clé d'activation et de serveur mandataire sont utilisées lors de l'installation manuelle.

Avant l'installation, configurez les variables requises dans le fichier de configuration utilisateur :

Procedure

Étape 1 Pour récupérer votre clé d'activation, accédez à **Manage(Gestion)** > **Agents**, cliquez sur l'onglet**Installer** (Installateur) , cliquez sur **Manual Install using classic packaged installers** (Installation manuelle à l'aide d'installateurs classiques), puis cliquez sur **Agent Activation Key** (Clé d'activation de l'agent).

Étape 2 Ouvrez le fichier `user.cfg` dans le dossier d'installation de l'agent Cisco Secure Workload. (Exemple : `/usr/local/tet` sous Linux ou `C:\\Program Files\\Cisco Tetration` sous Windows). Le fichier contient une liste de variables sous la forme « clé=valeur », une sur chaque ligne.

Étape 3 Ajoutez la clé d'activation à la variable **ACTIVATION_KEY**. Exemple : `ACTIVATION_KEY=7752163c635ef62e6568e9e852d07bd21bfd60d0`

Étape 4 Si l'agent nécessite un serveur mandataire HTTPS, ajoutez le serveur mandataire du protocole **http** et le port à l'aide de la variable **HTTPS_PROXY**. Exemple : `HTTPS_PROXY=http://proxy.my-company.com:80`

Other Agent-Like Tools

AnyConnect agents

Platforms supported by Cisco AnyConnect Secure Mobility agent with Network Visibility Module (NVM). No additional Cisco Secure Workload agent is required. AnyConnect connector registers these agents and exports flow observations, inventories, and labels to Cisco Secure Workload. For more information, please refer to AnyConnect Connector.

For Windows, Mac, or Linux platforms, please refer to Cisco AnyConnect Secure Mobility Client Data Sheet.

ISE agents

Endpoints registered with Cisco Identity Services Engine (ISE). No Cisco Secure Workload agent on the endpoint is required. ISE connector collects metadata about endpoints from ISE through pxGrid service on ISE appliance. It registers the endpoints as ISE agents on Cisco Secure Workload and pushes labels for the inventories on these endpoints. For more information, please refer to ISE Connector.

SPAN agents

SPAN agents work with the ERSPAN connector. For information, see Connecteur ERSPAN.

Integration with third-party and additional Cisco products

- Integrations using external orchestrators configured in Cisco Secure Workload.

  See Orchestrateurs externes dans Cisco Secure Workload, on page 125.

- Integrations using connectors configured in Cisco Secure Workload.

  See Que sont les connecteurs.

Renseignements sur la connectivité

En général, lorsque l'agent est installé sur le charges de travail, il établit plusieurs connexions réseau aux services principaux hébergés sur la grappe Cisco Secure Workload. Le nombre de connexions varie selon le type d'agent et ses fonctions.

Le tableau suivant présente les différentes connexions permanentes établies par les différents types d'agents.

Table 3: Connectivité des agents

Type d'agent	Serveur de configuration	Collecteurs	Serveur principal d'application
Visibilité (sur site)	CFG-SERVER-IP:443	COLLECTOR-IP:5640	S. O.
visibilité (logiciel-service SaaS)	CFG-SERVER-IP:443	COLLECTOR-IP:443	S. O.
des politiques de sécurité (sur site)	CFG-SERVER-IP:443	COLLECTOR-IP:5640	ENFORCER-IP:5660
enforcement (SaaS)	CFG-SERVER-IP:443	COLLECTOR-IP:443	ENFORCER-IP:443
images de Docker	CFG-SERVER-IP:443	s.o.	s.o.

Légende :

- CFG-SERVER-IP est l'adresse IP du serveur de configuration.
- COLLECTOR-IP est l'adresse IP du collecteur. Les agents de visibilité approfondie et d'application se connectent à tous les collecteurs disponibles.
- ENFORCER-IP est l'adresse IP du point terminal de mise en application. L'agent d'application se connecte à un seul des points terminaux disponibles.
- Pour les déploiements d'agents Kubernetes/OpenShift, le script d'installation ne contient pas le logiciel agent – Les images Docker contenant le logiciel agent sont extraites de la grappe Cisco Secure Workload par chaque nœud Kubernetes/OpenShift. Ces connexions sont établies par le composant de récupération de l'image de l'exécution du conteneur et dirigées vers CFG-SERVER-IP:443.

Accédez à **Platform** (Plateforme) > **Cluster Configuration** (Configuration de la grappe) pour connaître l'adresse IP du serveur de configuration et l'adresse IP du collecteur.

- **VIP de capteur** est l'adresse IP du serveur de configuration : l'adresse IP qui a été configurée pour le serveur de configuration dans cette grappe.
- **Les adresses IP externes** sont destinées aux adresses IP des collecteurs et à l'appareil de mise en application : si ce champ est rempli, lors de l'attribution d'adresses IP de grappe externe, le processus de sélection est limité aux adresses IP définies dans cette liste, qui font partie du réseau externe.

Note

- L'agent Cisco Secure Workload agit toujours en tant que client pour lancer les connexions aux services hébergés dans la grappe et n'ouvre jamais de connexion en tant que serveur.
- Les agents, pour lesquels la mise à niveau est prise en charge, effectuent périodiquement des requêtes HTTPS (port 443) auprès de la VIP de capteur de grappe pour connaître les paquets disponibles.
- Un agent peut être situé derrière un serveur NAT.

Les connexions à la grappe peuvent être refusées si la charge de travail est derrière un pare-feu, ou si le service de pare-feu de l'hôte est activé. Dans de tels cas, les administrateurs doivent créer des politiques de pare-feu appropriées pour autoriser les connexions.

Exclusions de sécurité

Les agents logiciels interagissent en permanence avec le système d'exploitation de l'hôte dans le cadre de leurs activités normales. Par conséquent, d'autres applications de sécurité installées sur l'hôte, comme les antivirus, les agents de sécurité et autres, pourraient déclencher des alertes ou bloquer les actions des agents Cisco Secure Workload. C'est pourquoi, pour vous assurer que les agents sont installés avec succès et fonctionnent, vous devez configurer les exclusions de sécurité nécessaires sur les applications de sécurité qui surveillent l'hôte.

Table 4: Exclusions de sécurité pour les répertoires d'agents

Système d'exploitation de l'hôte	Répertoires
AIX	/opt/cisco/tetration
Linux	/usr/local/tet or /opt/cisco/tetration or <user chosen inst dir>
	/var/opt/cisco/secure-workload
Windows	C:\Program Files\Cisco Tetration
	C:\ProgramData\Cisco Tetration
Solaris	/opt/cisco/secure-workload

Table 5: Exclusions de sécurité pour les processus d'agent

Système d'exploitation de l'hôte	Processus
AIX	tet-engine, tet-sensor, tet-enforcer
Linux	tet-engine, tet-sensor, tet-enforcer, tet-main, enforcer
Windows	TetSenEngine.exe, TetSen.exe, TetEnfEgine.exe, TetEnfC.exe, TetEnf.exe, TetUpdate.exe, tet-main.exe

Table 6: Exclusions de sécurité pour les processus d'agent

Système d'exploitation de l'hôte	Processus
AIX	tet-engine, tet-sensor, tet-enforcer
Linux	tet-engine, tet-sensor, tet-enforcer, tet-main, enforcer
Windows	CswEngine.exe, TetEnfC.exe

Table 7: Exclusions de sécurité pour les processus d'agent

Système d'exploitation de l'hôte	Processus
AIX	csw-agent
	tet-sensor
	tet-enforcer
	tet-main
Linux	csw-agent
	tet-sensor
	tet-enforcer
	tet-main
	exécuteur
Windows	TetSenEngine.exe
	TetSen.exe
	TetEnfEgine.exe
	TetEnfC.exe
	TetEnf.exe
	TetUpdate.exe
	tet-main.exe
Solaris	csw-agent
	tet-sensor
	tet-main

Table 8: Exclusions de sécurité pour les processus d'agent

Système d'exploitation de l'hôte	Processus
AIX	csw-agent
	tet-sensor
	tet-enforcer
	tet-main

Système d'exploitation de l'hôte	Processus
Linux	csw-agent
	tet-sensor
	tet-enforcer
	tet-main
	exécuteur
Windows	CswEngine.exe
	TetEnfC.exe
Solaris	csw-agent
	tet-sensor
	tet-enforcer
	tet-main

Table 9: Exclusions de sécurité pour les actions des agents

Système d'exploitation de l'hôte	Actions
AIX	Access /dev/bpf*, /dev/ipl, /dev/kmem
	Invokes cfg_ipf, curl, ipf, ippool, ipfstat lslpp, lsfilt, prtconf
	Scan /proc
Linux	Invokes curl, ip[6]tables-save, ip[6]tables-restore, rpm/dpkg
	Scan /proc, open netlink sockets
Windows	Accéder au registre
	S'inscrire aux événements du pare-feu
	Invokes c:\windows\system32\netsh.exe
Solaris	Invokes curl, lspp, pkg, smbios
	Scan /proc

Table 10: Exclusions de sécurité pour les scripts d'agent ou les exécutions binaires

Système d'exploitation de l'hôte	Scripts/binaires appelés
AIX	-

Système d'exploitation de l'hôte	Scripts/binaires appelés
Linux	-
Windows	dmidecode.exe
	npcap-installer.exe
	sensortools.exe
	signtool.exe
Solaris	-

Gestion des services des agents

Les agents logiciels sont déployés en tant que service sur toutes les plateformes prises en charge. Cette section décrit des méthodes de gestion des services pour diverses fonctions et plateformes.

Note Sauf indication contraire, toutes les commandes de cette section nécessitent des privilèges racine sur Linux ou Unix, ou des privilèges d'administration sur Windows pour s'exécuter.

Gestion des services pour RHEL, CentOS, OracleLinux-6.x et Ubuntu-14

Exécutez les commandes suivantes pour :

- **Démarrer un service** : `start csw-agent`
- **Arrêter un service** : `stop csw-agent`
- **Redémarrer un service** : `restart csw-agent`
- **Vérifier l'état du service** : `status csw-agent`

Gestion des services pour RHEL, CentOS, OracleLinux-7.x et versions ultérieures

Les commandes sont également applicables à :

- AlmaLinux, Rocky Linux – 8.x et versions ultérieures
- Amazon Linux 2 ou versions ultérieures
- Debian 8 et versions ultérieures
- SLES-12SPx et versions ultérieures
- Ubuntu-16.04 et versions ultérieures

Exécutez les commandes suivantes pour :

- **Démarrage d'un service** : `systemctl start csw-agent`
- **Arrêt d'un service** : `systemctl stop csw-agent`
- **Redémarrage d'un service** : `systemctl restart csw-agent`
- **Vérification de l'état du service** : `systemctl status csw-agent`

Gestion des services pour Windows Server ou Windows VDI

Exécutez les commandes suivantes pour :

- **Démarrage d'un service** : `net start <nom du service>`

  Exemple : **net start tetsensor** pour le service de visibilité approfondie - **net start tetenforcer** pour le service d'application

  Exemple : **net start cswagent** pour le service de visibilité approfondie et d'application

- **Arrêter un service** : `net stop<nom du service>`

  Exemple : **net stop tetsensor** pour le service de visibilité approfondie - **net stop tetenforcer** pour le service de mise en application

  Exemple : **net stop cswagent** pour une visibilité approfondie et le service d'application

- **Redémarrage d'un service** :

  1. `net stop <nom du service>`
  2. `net start <nom du service>`

- **Vérification de l'état du service** : `sc query<nom du service>`

  Exemple : **sc query tetsensor** pour le service de visibilité approfondie - **sc query tetenforcer** pour le service de mise en application

  Exemple : **sc query cswagent** pour un service de visibilité approfondie et d'application

Gestion des services pour AIX

Exécutez les commandes suivantes pour :

- **Démarrage d'un service** : `startsrc -s csw-agent`
- **Arrêt d'un service** : `stopsrc -s csw-agent`
- **Redémarrage d'un service** :

  1. `stopsrc -s csw-agent`
  2. `startsrc -s csw-agent`

- **Vérification de l'état du service** : `lssrc -s csw-agent`

Gestion du service pour les installations d'agents Kubernetes

- **Démarrage ou arrêt d'un service** : il n'est pas possible de démarrer ou d'arrêter les agents sur un nœud en particulier, car ils ne sont pas installés en tant que services individuels, mais en tant qu'ensemble de daemons à l'échelle de la grappe.
- **Redémarrage d'un agent sur un nœud** : Localisez le pod d'agents Cisco Secure Workload sur le nœud et exécutez la commande Kubernetes appropriée pour l'arrêter. Le pod est redémarré automatiquement.
- **Vérification de l'état des pods**: `kubectl get pod -n tetration` or `oc get pod -n tetration` (for OpenShift) répertorie l'état de tous les pods d'agents Cisco Secure Workload dans la grappe Kubernetes.

Gestion des services pour Solaris

Exécutez les commandes suivantes pour :

- **Démarrer un service** : `svcadm enable csw-agent`
- **Arrêter un service** : `svcadm disable csw-agent`
- **Redémarrer un service** : `svcadm restart csw-agent`
- **Vérifier l'état du service** : `svcs -l csw-agent`

Application des politiques par le biais d'agents

Par défaut, les agents installés sur vos charges de travail ont la capacité d'appliquer des politiques, mais l'application est désactivée. Lorsque vous êtes prêt, vous pouvez activer ces agents pour appliquer les politiques sur les hôtes sélectionnés en fonction de l'intent configuré.

Lorsqu'un agent applique une politique, il applique un ensemble ordonné de règles qui spécifient si le pare-feu doit AUTORISER ou ABANDONNER un trafic réseau spécifique en fonction de paramètres tels que la source, la destination, le port, le protocole et la direction. Pour en savoir plus sur les politiques, consultez Gérer le cycle de vie des politiques dans Cisco Secure Workload, on page 429.

Mise en application utilisant des agents

- Les agents reçoivent les politiques sur un canal TCP ou SSL sécurisé.
- Les agents s'exécutent dans un domaine privilégié. Sur les machines Linux, l'agent s'exécute en tant qu'utilisateur « root »; sur les machines Windows, l'agent s'exécute en tant que SYSTEM.
- Selon la plateforme, lorsque l'application des politiques est activée, les agents peuvent contrôler complètement le pare-feu ou utiliser les règles configurées existantes.
- Pour en savoir plus sur les options d'application et pour activer et configurer les agents afin d'appliquer les politiques, consultez Creating an Agent Config Profile, on page 83.

Détails avancés

Lorsque vous activez l'application, des règles d'or sont formulées pour permettre à l'agent de se connecter au contrôleur. Les agents communiquent avec Enforcement Front End (EFE) du contrôleur par l'intermédiaire

d’un canal bidirectionnel sécurisé utilisant le protocole TLS ou SSL. Les messages du contrôleur sont signés par le générateur de politiques et vérifiés par l’agent.

L’agent reçoit les politiques du contrôleur dans un schéma indépendant de la plateforme. L’agent convertit ces politiques indépendantes de la plateforme en politiques spécifiques à la plateforme et programme le pare-feu sur le point terminal.

L’agent surveille activement l’état du pare-feu. Si l’agent détecte un écart dans les politiques appliquées, il applique à nouveau les politiques mises en cache dans le pare-feu. L’agent surveille également sa propre consommation de ressources système, telles que le processeur et la mémoire.

L’agent envoie régulièrement un rapport d’état et de statistiques au contrôleur à l’aide d’EFE. Le rapport d’état comprend l’état des dernières politiques programmées telles que la réussite, l’échec ou l’erreur, le cas échéant. Le rapport de statistiques comprend les statistiques de politique telles que les paquets autorisés et abandonnés, et le nombre d’octets selon la plateforme.

Application par les agents sur la plateforme Linux

Sur la plateforme Linux, l’agent utilise des iptables, ip6tables ou ipset pour appliquer les politiques de réseau. Une fois l’agent activé sur l’hôte, il contrôle et programme les iptables par défaut. Si la pile réseau IPv6 est activée, l’agent contrôle le pare-feu IPv6 à l’aide des ip6tables.

iptables ou ip6tables Linux

Le noyau Linux dispose de iptables et ip6tables qui sont utilisés pour configurer, maintenir et inspecter les tableaux de règles de filtrage de paquets IPv4 et IPv6. Ces iptables et ip6tables se composent de nombreux tableaux prédéfinis. Chaque tableau contient des chaînes prédéfinies et peut également contenir des chaînes définies par l'utilisateur. Ces chaînes contiennent des ensembles de règles et chacune de ces règles spécifie les critères de correspondance pour un paquet. Les tableaux prédéfinis sont les suivants : raw, mangle, filter et NAT. Les chaînes prédéfinies sont INPUT, OUTPUT, FORWARD, PREROUTING et POSTROUTING.

L’agent Cisco Secure Workload programme une table de filtres qui contient des règles pour autoriser ou abandonner les paquets. La table de filtres comprend les chaînes prédéfinies INPUT, OUTPUT et FORWARD. En outre, l'agent ajoute des chaînes d'assistance technique (AT) personnalisées pour classer et gérer les politiques du contrôleur. Ces chaînes d’assistance technique contiennent des règles Cisco Secure Workload dérivées des politiques ainsi que des règles générées par l’agent. Lorsque l’agent reçoit des règles indépendantes de la plateforme, il les analyse et les convertit en règles iptable, ip6table ou ipset et insère ces règles dans les chaînes définies par l'AT dans la table de filtrage. Après avoir programmé le pare-feu, l’agent le surveille pour détecter tout écart aux règles ou aux politiques et, si c’est le cas, le reprogrammer. Il effectue le suivi des politiques programmées dans le pare-feu et communique régulièrement leurs statistiques au contrôleur.

Voici un exemple illustrant ce comportement :

Une politique typique dans un message de politique de réseau indépendant de la plateforme se compose des éléments suivants :

```
source set id: “test-set-1”
destination set id: “test-set-2”
source ports: 20-30
destination ports: 40-50
ip protocol: TCP
action: ALLOW
. . .
set_id: “test-set-1”
     ip_addr: 1.2.0.0
     prefix_length: 16
     address_family: IPv4
```

```
set_id: "test-set-2"
     ip_addr: 3.4.0.0
     prefix_length: 16
     address_family: IPv4
```

Avec d'autres informations, l'agent traite cette politique et la convertit en règles ipset et iptables spécifiques à la plateforme :

```
ipset rule:
Name: ta_f7b05c30ffa338fc063081060bf3
Type: hash:net
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 16784
References: 1
Members:
1.2.0.0/16
Name: ta_1b97bc50b3374829e11a3e020859
Type: hash:net
Header: family inet hashsize 1024 maxelem 65536
Size in memory: 16784
References: 1
Members:
3.4.0.0/16
iptables rule:
TA_INPUT -p tcp -m set --match-set ta_f7b05c30ffa338fc063081060bf3 src -m set --match-
‹→set ta_1b97bc50b3374829e11a3e020859 dst -m multiport --sports 20:30 -m multiport --
‹→dports 40:50 -j ACCEPT
```

Mises en garde

Module de noyau ipset

Lorsque la mise en application est activée et que la conservation des règles est désactivée dans le profil de configuration de l'agent, les agents exécutés sur des hôtes Linux veillent à ce que le module de noyau ipset ait une configuration *max_sets* de valeur suffisante. Au cas où une modification est nécessaire, l'agent recharge le module de noyau ipset avec une nouvelle valeur *max_sets* . Si Preserve Rules (Conserver règles) est activé, les agents vérifient la valeur *max_sets* du module ipset, mais n'apportent aucune modification. La valeur *max_sets* actuellement configurée se trouve dans `cat /sys/module/ip_set/parameters/max_sets`.

Sauvegarde du pare-feu de l'hôte

La première fois que cette application est activée dans le profil de configuration de l'agent, les agents exécutés sur des hôtes Linux stockent le contenu actuel des tableaux ipset et ip6(6) dans `/opt/cisco/tetration/backup` avant de prendre le contrôle du pare-feu de l'hôte.

Les transitions successives pour activer ou désactiver la configuration d'application ne génèrent pas de sauvegardes. Le répertoire n'est pas supprimé après la désinstallation de l'agent.

Application par les agents sur la plateforme Windows en mode WAF

Sur la plateforme Windows, l'agent Cisco Secure Workload utilise le pare-feu Windows pour appliquer les politiques de réseau.

Pare-feu Windows avec sécurité avancée

Un composant natif de Windows, le Pare-feu avec fonctions de sécurité Windows, régule le trafic réseau en fonction des types de paramètres suivants :

- Les règles qui régissent le trafic réseau entrant.
- Les règles qui régissent le trafic réseau sortant.
- Remplacer les règles basées sur l'état d'authentification de la source et de la destination du trafic réseau.
- Règles qui s'appliquent au trafic IPsec et aux services Windows.

La politique réseau Cisco Secure Workload est programmée à l'aide de règles de pare-feu de trafic entrant et sortant.

Règles Cisco Secure Workload et pare-feu Windows

Sur la plateforme Windows, la politique réseau Cisco Secure Workload est appliquée comme suit :

1. Les règles de pare-feu indépendantes de la plateforme de la politique réseau Cisco Secure Workload sont converties en règles de pare-feu Windows.
2. Les règles sont programmées dans le pare-feu Windows.
3. Le pare-feu Windows applique les règles.
4. Le pare-feu Windows et son ensemble de règles sont surveillés. Si un changement est détecté, l'écart est signalé et la politique du réseau Cisco Secure Workload est réinitialisée dans le pare-feu Windows.

Profils de sécurité

Le pare-feu Windows regroupe les règles en fonction du réseau auquel l'hôte est connecté. Ces groupes de règles sont appelés profils, et il existe trois profils de ce type :

- Profil de domaine
- Profil privé
- Profil public

Les règles Cisco Secure Workload sont programmées dans tous les profils, mais seules les règles des profils actifs sont surveillées en permanence.

Politiques de paramètres et de listes mixtes en vigueur

L'ensemble de règles du pare-feu Windows n'est pas classé en fonction de la priorité. Lorsque plusieurs règles correspondent à un paquet, les plus restrictives de ces règles prennent effet, ce qui signifie que les règles DENY (REFUSER) prévalent sur les règles ALLOW (AUTORISER). Pour en savoir plus, consultez l'article sur Microsoft TechNet.

Prenons l'exemple de la politique de liste mixte (autorisation et refus) de la section sur l'agent d'application :

```
1. ALLOW 1.2.3.30 tcp port 80
2. ALLOW 1.2.3.40 udp port 53
3. BLOCK 1.2.3.0/24 ip
4. ALLOW 1.2.0.0/16 ip
5. Catch-all: DROP ingress, ALLOW egress
```

Lorsqu'un paquet à destination du port TCP 80 1.2.3.30 de l'hôte atteint le pare-feu, il correspond à toutes les règles, mais la plus restrictive de toutes, la règle numéro 3, est celle qui sera appliquée et le paquet sera abandonné. Ce comportement est contraire à l'attente selon laquelle les règles seront évaluées dans l'ordre, la règle 1 est la règle qui est appliquée et le paquet sera autorisé.

Cette différence de comportement est à prévoir sur la plateforme Windows en raison de la conception du pare-feu Windows décrite ci-dessus. Ce comportement peut être observé dans les politiques de listes mixtes avec des règles qui se chevauchent qui ont différentes actions liées.

Par exemple :

```
1. ALLOW 1.2.3.30 tcp
2. BLOCK 1.2.3.0/24 tcp
```

Interférence provenant d'autres pare-feu ou politiques

Nous vous recommandons d'accorder à l'agent le contrôle total et exclusif du pare-feu Windows pour appliquer la politique réseau Cisco Secure Workload comme prévu. Les agents ne peuvent pas appliquer la politique de manière fiable dans les cas suivants :

- Un pare-feu tiers est présent. (Le pare-feu Windows doit être le produit de pare-feu actif sur l'hôte).
- Le pare-feu est désactivé pour les profils actuels.
- Des paramètres de pare-feu en conflit sont déployés à l'aide de la politique de groupe. Voici certains des paramètres en conflit :
  - Règles de pare-feu
  - Actions entrantes ou sortantes par défaut dans les profils actuels qui diffèrent des règles globales de la politique.
  - Pare-feu désactivé pour les profils actuels

Application par état

Le pare-feu avancé Windows est considéré comme un pare-feu **par état**, c'est-à-dire que pour certains protocoles comme TCP, le pare-feu maintient un suivi d'état interne pour détecter si un nouveau paquet touchant le pare-feu appartient à une connexion connue. Les paquets appartenant à une connexion connue sont autorisés sans qu'il soit nécessaire d'examiner les règles du pare-feu. Un pare-feu par état permet la communication bidirectionnelle sans qu'il soit nécessaire d'établir des règles dans les tables INBOUND et OUTBOUND (entrée et sortie).

Par exemple, imaginons la règle suivante pour un serveur Web : **accepter toutes les connexions TCP sur le port 443**

L'intention est d'accepter toutes les connexions TCP sur le port 443 avec le serveur et de permettre au serveur de communiquer avec les clients. Dans ce cas, une seule règle est insérée dans la table INBOUND, autorisant les connexions TCP sur le port 443. Aucune règle ne doit être insérée dans la table OUTBOUND. L'insertion d'une règle dans la table OUTBOUND est effectuée implicitement par le pare-feu avancé de Windows.

Note Le suivi avec état s'applique uniquement aux protocoles qui établissent et gèrent des connexions explicites. Pour les autres protocoles, les règles d'entrée et de sortie doivent être programmées pour activer la communication bidirectionnelle.

Lorsque l'application est activée, une règle concrète est programmée comme **par état** lorsque le protocole est TCP (l'agent décide, en fonction du contexte, si la règle doit être insérée dans la table INBOUND ou dans la table OUTBOUND). Pour les autres protocoles (y compris **ANY**), les règles INBOUND et OUTBOUND sont toutes deux programmées.

Mises en garde

Sauvegarde du pare-feu de l'hôte

Lorsque l'application est activée pour la première fois dans le profil Agent Config (Configuration de l'agent), les agents exécutés sur des hôtes Windows, avant de prendre le contrôle du pare-feu de l'hôte, exportent le contenu actuel du pare-feu avancé Windows vers `ProgramData\Cisco\Tetration\backup`. Les transitions successives pour activer ou désactiver la configuration d'application ne génèrent pas de sauvegardes. Le répertoire n'est pas supprimé lors de la désinstallation de l'agent.

Mise en application par les agents sur la plateforme Windows en mode WFP

Sur la plateforme Windows, l'agent applique les politiques de réseau en programmant des filtres de la plateforme de filtrage Windows (WFP). Le pare-feu avancé Windows n'est pas utilisé pour configurer la politique de réseau.

Plateforme de filtrage Windows

La plateforme de filtrage Windows (WFP) est un ensemble d'API fourni par Microsoft pour configurer des filtres de traitement du trafic réseau. Les filtres de traitement du trafic réseau sont configurés à l'aide d'API au niveau du noyau et des API au niveau de l'utilisateur. Les filtres WFP peuvent être configurés selon différentes couches, notamment la couche réseau, la couche de transport ou l'application de la couche applicative (ALE). Les filtres WFP Cisco Secure Workload sont configurés au niveau de la couche ALE, de manière similaire aux règles de pare-feu Windows. Chaque couche comporte plusieurs sous-couches, classées par pondération, de la plus élevée à la plus faible. Dans chaque sous-couche, les filtres sont classés par pondération, du plus élevé au plus bas. Un paquet réseau traverse toutes les sous-couches. À chaque sous-couche, les paquets réseau passent par les filtres correspondants en fonction de la pondération, de la plus élevée à la plus faible, et renvoient l'action : Autoriser ou Bloquer. Après avoir traversé toutes les sous-couches, le paquet est traité en fonction de la règle selon laquelle l'action de blocage prévaut sur l'autorisation.

Avantages de WFP par rapport à WAF

- Évite les dépendances de configuration du pare-feu Windows.
- Surmonte les restrictions des GPO.
- Assure la facilité de la migration et du renversement des politiques.
- Vous permet de contrôler l'ordre des politiques.
- Évite l'ordre strict de la politique de blocage en premier du pare-feu Windows.
- Réduit la surcharge du CPU lors de la mise à jour de la politique.
- Crée un filtre de règles de politique unitaire efficace.
- Assure une mise à jour plus rapide en une seule étape.

Prise en charge des agents pour WFP

Lorsque l'application est configurée pour utiliser WFP, les filtres Cisco Secure Workload remplacent les règles du pare-feu Windows.

En mode WFP, l'agent configure les objets WFP suivants :

- Le fournisseur a un GUID et un nom, est utilisé pour la gestion des filtres et n'affecte pas le filtrage de paquets
- La sous-couche a un GUID, un nom et une pondération. La sous-couche de Cisco Secure Workload est configurée avec une pondération plus élevée que la sous-couche Windows Advanced Firewall.
- Le filtre comporte un nom, un GUID, un ID, une pondération, un ID de couche, une clé de sous-couche, une action (PERMIT/BLOCK) et des conditions. Les filtres WFP sont configurés pour les règles Golden, les règles automatiques et les règles de politique. L'agent configure également les filtres de prévention du balayage de ports. Les filtres de Cisco Secure Workload sont configurés avec l'indicateur FWPM_FILTER_FLAG_CLEAR_ACTION_RIGHT. Cet indicateur garantit que les filtres de Cisco Secure Workload ne sont pas remplacés par les règles de pare-feu Microsoft. Pour chaque règle de politique de réseau Cisco Secure Workload, un ou plusieurs filtres WFP sont configurés en fonction de la direction (entrante ou sortante) et du protocole.

Pour la politique du trafic entrant TCP,

```
id: 14 , TCP Allow 10.195.210.184 Dir=In localport=3389
```

les filtres WFP configurés sont les suivants :

```
Filter Name:                  Cisco Secure Workload Rule 14
-----------------------------------------------------
EffectiveWeight:                        18446744073709551589
LayerKey:                               FWPM_LAYER_ALE_AUTH_LISTEN_V4
Action:                                 Permit
Local Port:                             3389
Filter Name:                            Cisco Secure Workload Rule 14
-----------------------------------------------------
EffectiveWeight:                        18446744073709551589
LayerKey:                               FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                                 Permit
RemoteIP:                               10.195.210.184-10.195.210.184
```

L'agent Cisco Secure Workload configure les filtres **entrant par défaut Secure Workload** et **sortant par défaut Secure Workload** pour la politique CATCH-ALL (COLLECTRICE) entrante et sortante, respectivement.

Prise en charge WFP de l'agent et pare-feu Windows

- L'agent **ne surveille pas** les règles WAF, ni les profils WAF.
- L'agent **ne surveille pas** les états du pare-feu.
- L'agent **ne nécessite pas** l'activation de l'état du pare-feu.
- L'agent **n'est pas en conflit** avec les politiques des objets de politique de groupe (GPO).

Politiques de paramètres et de listes mixtes en vigueur

La mise en application des agents en mode WFP prend en charge les politiques de listes mixtes ou grisées.

Prenons l'exemple de la politique de liste mixte (autorisation et refus) de la section sur l'agent d'application :

```
1. ALLOW 1.2.3.30 tcp port 80-            wt1000
2. BLOCK 1.2.3.0/24 ip-                   wt998
3. ALLOW 1.2.0.0/16 ip-                   wt997
4. Catch-all: DROP ingress, ALLOW egress - wt996
```

Lorsqu'un paquet à destination du port 80 1.2.3.30 de l'hôte atteint le pare-feu, il correspond au filtre 1 et est autorisé. Cependant, un paquet à destination de l'hôte 1.2.3.10 est bloqué à cause du filtre 2. Un paquet qui se dirige vers l'hôte 1.2.2.10 est autorisé par le filtre 3.

Application par état

Les filtres WFP de Cisco Secure Workload sont configurés au niveau de la couche ALE. Le trafic réseau est filtré pour les opérations socket connect(), listen() et accept(). Les paquets réseau associés à une connexion L4 ne sont pas filtrés après l'établissement de la connexion.

Visibilité des filtres WFP configurés

Vous pouvez afficher les filtres WFP configurés Cisco Secure Workload à l'aide de `c:\program files\tetration\tetenf.exe`. Les options prises en charge sont les suivantes :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `c:\program files\tetration\tetenf.exe -l -f <-verbose> <-output=outfile.txt>`.

OU

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Affichez le fichier **filters.xml** pour connaître les filtres Cisco Secure Workload configurés.

Désactiver les filtres du mode furtif en mode WFP

Pour désactiver les filtres de mode furtif (filtres d'analyse de ports) :

Procédure

Étape 1 Modifiez `\conf\enforcer.cfg`.

Étape 2 Ajoutez **disable_wfp_stealth_mode**: 1

Étape 3 Enregistrez le fichier.

Étape 4 Avec des privilèges d'administration, redémarrez le service tetenforcer en :

a) Exécutant la commande : `sc stop tetenforcer` to stop TetEnforcer Service.
b) Exécutant la commande : `sc start tetenforcer` to start TetEnforcer Service.

Étape 5 Avec des privilèges d'administration, redémarrez le service CswAgent en :

a) Exécutant la commande : `sc stop cswagent` pour arrêter le service CswAgent.
b) Exécutant la commande : `sc start cswagent` pour démarrer le service CswAgent.

Étape 6 Pour vérifier :

a) Avec des privilèges d'administration, exécutez `cmd.exe`.
b) Exécutant la commande : `c:\program files\tetration\tetenf.exe -l -f <-verbose> <-output=outfile.txt>`.

```
"Tetration Internal Rule block portscan" filters are not configured.
```

Supprimer les filtres WFP configurés

Vous pouvez supprimer les filtres WFP Cisco Secure Workload configurés à l'aide de `c:\program files\tetration\tetenf.exe`. Pour éviter la suppression accidentelle de filtres, lorsque vous exécutez la commande de suppression, spécifiez le jeton au format <*yyyymm*>, où *yyyy* est l'année en cours et *mm* est le mois en cours sous forme numérique. Par exemple, si la date du jour est le 21/01/2021, le jeton est **-token=202101**

Les options prises en charge sont les suivantes :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Pour supprimer tous les filtres Cisco Secure Workload configurés, exécutez `c:\program files\tetration\tetenf.exe -d -f -all - token=<yyyymm>`
- Pour supprimer tous les objets Cisco Secure Workload WFP configurés, exécutez `c:\program files\tetration\tetenf.exe -d -all -token=<yyyymm>`
- Pour supprimer un filtre Cisco Secure Workload WFP par nom, exécutez `c:\program files\tetration\tetenf.exe -d -name=<WFP filter name> -token=<yyyymm>`

Limites connues du mode WFP

- Le paramètre **Preserve Rules** (Conserver les règles) du profil de configuration de l'agent n'a aucun effet lorsque vous définissez le mode d'application sur WFP.

Configurer les politiques pour les attributs Windows

Pour plus de granularité lors de l'application d'une politique sur les charges de travail basées sur Windows, vous pouvez filtrer le trafic réseau par :

- Nom de l'application
- Nom du service
- Noms d'utilisateur avec ou sans groupes d'utilisateurs

Cette option est prise en charge dans les modes WAF et WFP. Les filtres basés sur le système d'exploitation Windows sont classés en tant que *filtres de consommateur* et de *filtres de fournisseur* dans la politique de réseau générée. Les filtres des consommateurs filtrent le trafic réseau qui est initié par la charge de travail des consommateurs et les filtres des fournisseurs filtrent le trafic réseau qui est destiné au travail du fournisseur.

Avant de commencer

Cette procédure suppose que vous modifiez une politique existante. Si vous n'avez pas encore créé la politique à laquelle ajouter un filtre basé sur le système d'exploitation Windows, créez d'abord cette politique.

Important Consultez Mises en garde, à la page 67 et Limites connues, à la page 66 pour des renseignements sur les politiques impliquant les attributs Windows.

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Defend (Défendre)** > **Segmentation** .

Étape 2 Cliquez sur la portée qui contient la politique pour laquelle vous souhaitez configurer des filtres basés sur le système d'exploitation Windows.

Étape 3 Cliquez sur l'espace de travail dans lequel vous souhaitez modifier la politique.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

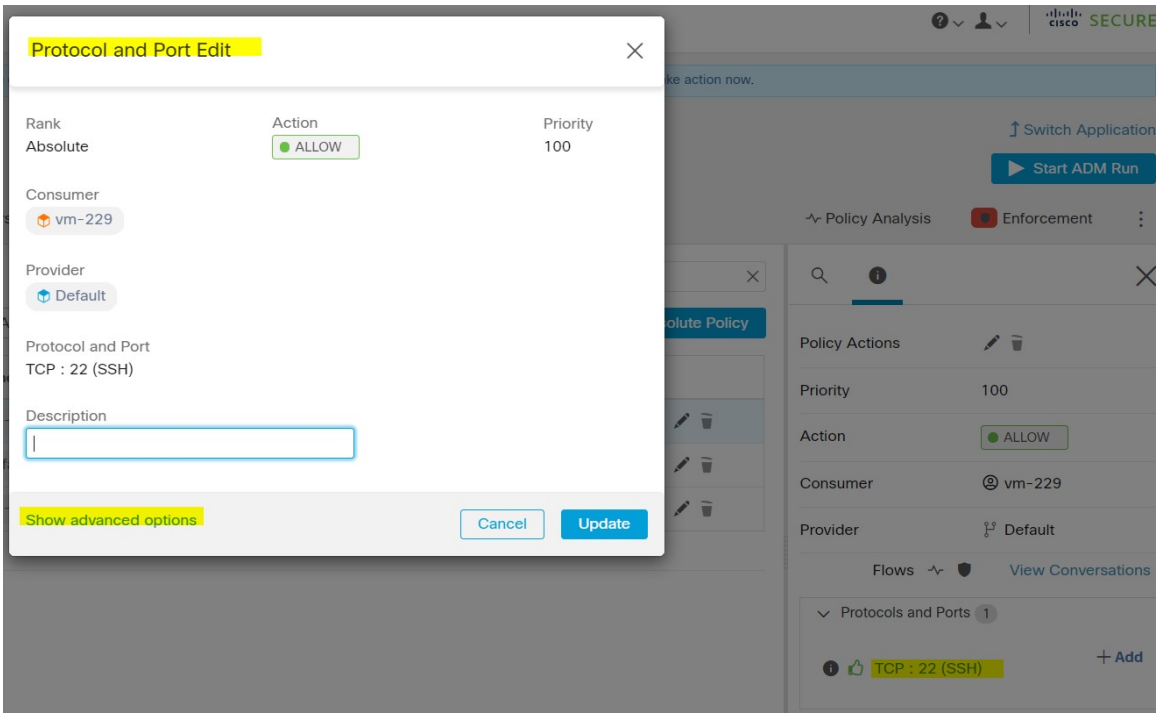
Étape 5 Choisissez la politique à modifier.

Important Le client et le fournisseur doivent inclure uniquement les charges de travail Windows.

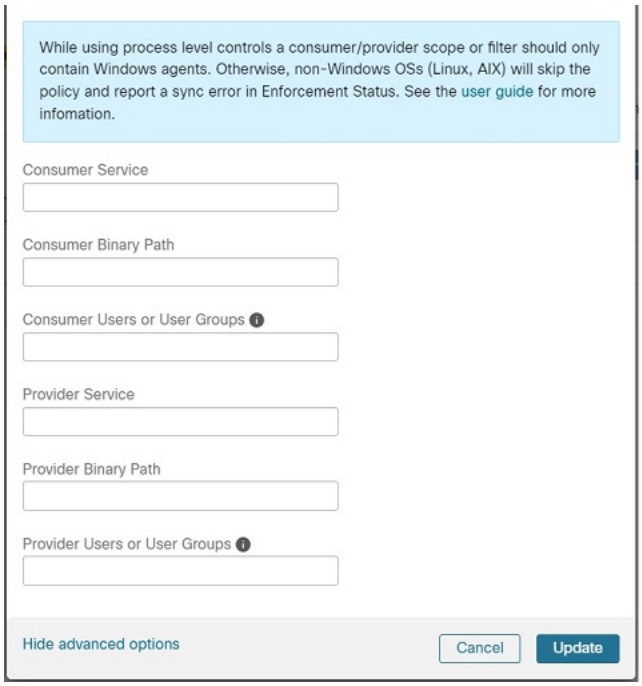
Étape 6 Dans la ligne du tableau permettant de modifier la politique, cliquez sur la valeur existante dans la colonne **Protocols and Ports** (protocoles et ports).

Étape 7 Dans le volet de droite, cliquez sur la valeur existante sous **Protocols and Ports**.

Dans l'exemple, cliquez sur **`TCP : 22 (SSH).`**



Étape 8 Cliquez sur **Show Advanced Options** (Afficher les options avancées).



Étape 9 Configurez les filtres de consommateur en fonction du nom de l'application, du nom du service ou du nom d'utilisateur.

- Le nom de l'application doit être un chemin d'accès complet.
- Le nom du service doit être un nom de service court.
- Le nom d'utilisateur peut être un nom d'utilisateur local (par exemple, tetter) ou un nom d'utilisateur de domaine (par exemple, capteur-dev@capteur-dev.com ou capteur-dev\capteur-dev)
- Le groupe d'utilisateurs peut être un groupe d'utilisateurs local (par exemple, Administrateurs) ou un groupe d'utilisateurs de domaine (par exemple, domaine utilisateurs\\capteur-dev)
- Plusieurs noms d'utilisateurs et/ou de groupes d'utilisateurs peuvent être spécifiés, séparés par « , » (par exemple, capteur-dev\@capteur-dev.com,utilisateurs du domaine\\capteur-dev)
- Le nom du service et le nom d'utilisateur ne peuvent pas être configurés ensemble.

Étape 10 Configurez les filtres de fournisseur en fonction du nom de l'application, du nom de service ou du nom d'utilisateur.

Suivez les mêmes directives que celles données à l'étape précédente pour les filtres du consommateur.

Étape 11 Saisissez les chemins d'accès au fichier binaire, le cas échéant.

Par exemple, saisissez `c:\test\putty.exe`

Étape 12 Cliquez sur **Update** (mettre à jour).

Configuration de politique basée sur le système d'exploitation Windows recommandée

toujours spécifier les ports et les protocoles dans les politiques, lorsque cela est possible; nous vous recommandons de ne permettre AUCUN port, AUCUN protocole.

Par exemple, une politique générée avec des restrictions de port et de protocole pourrait ressembler à ceci :

```
 dst_ports {
  start_port: 22
  end_port: 22
  consumer_filters {
    application_name: "c:\\test\\putty.exe"
  }
 }}
 ip_protocol: TCP
```

En revanche, si vous autorisez les connexions réseau lancées par iperf.exe avec TOUS les protocoles et TOUS les ports, la politique générée ressemblera à ceci :

```
match_set {
  dst_ports {
    end_port: 65535
    consumer_filters {
      application_name: "c:\\test\\iperf.exe"
    }
  }
  address_family: IPv4
  inspection_point: EGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Pour le filtre ci-dessus, Cisco Secure Workload crée une règle de politique pour autoriser le trafic réseau sur le fournisseur comme suit :

```
match_set {
    dst_ports {
    end_port: 65535
  }
  address_family: IPv4
  inspection_point: INGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Cette règle de réseau ouvre tous les ports sur le fournisseur. Nous vous déconseillons de créer des filtres basés sur le système d'exploitation avec le protocole *Any* (Tous).

Limites connues

- Windows 2008 R2 ne prend pas en charge les politiques de filtrage basées sur le système d'exploitation Windows.
- La politique de réseau peut être configurée avec un nom d'utilisateur unique, tandis que l'interface utilisateur du pare-feu Microsoft prend en charge plusieurs utilisateurs.

Mises en garde

- Lors de l'utilisation de politiques basées sur le système d'exploitation Windows, une portée ou un filtre consommateur ou fournisseur ne doit contenir que des agents Windows. Sinon, les systèmes d'exploitation autres que Windows (Linux, AIX) ignorent la politique et signalent une erreur de synchronisation dans l'état d'application.
- Évitez de créer des filtres de système d'exploitation Windows avec des critères de filtrage *peu rigoureux*. De tels critères peuvent ouvrir des ports réseau indésirables.
- Si les filtres de système d'exploitation sont configurés pour le client, les politiques ne s'appliquent qu'au client. De même, s'ils sont configurés pour le fournisseur, ils ne s'appliquent qu'au fournisseur.
- Étant donné que les connaissances relatives au contexte du processus, de l'utilisateur ou de service sont limitées ou inexistantes, il y aura des écarts dans l'analyse des politiques si elles comportent des filtres basés sur le système d'exploitation Windows.

Vérification et dépannage des politiques avec les attributs de filtrage basés sur le système d'exploitation Windows

Si vous utilisez des attributs de filtrage basés sur le système d'exploitation Windows, les rubriques suivantes vous fourniront des informations de vérification et de dépannage.

Le service d'assistance Cisco TAC peut utiliser ces informations au besoin pour effectuer le dépannage de ces politiques.

Politiques basées sur le nom de l'application

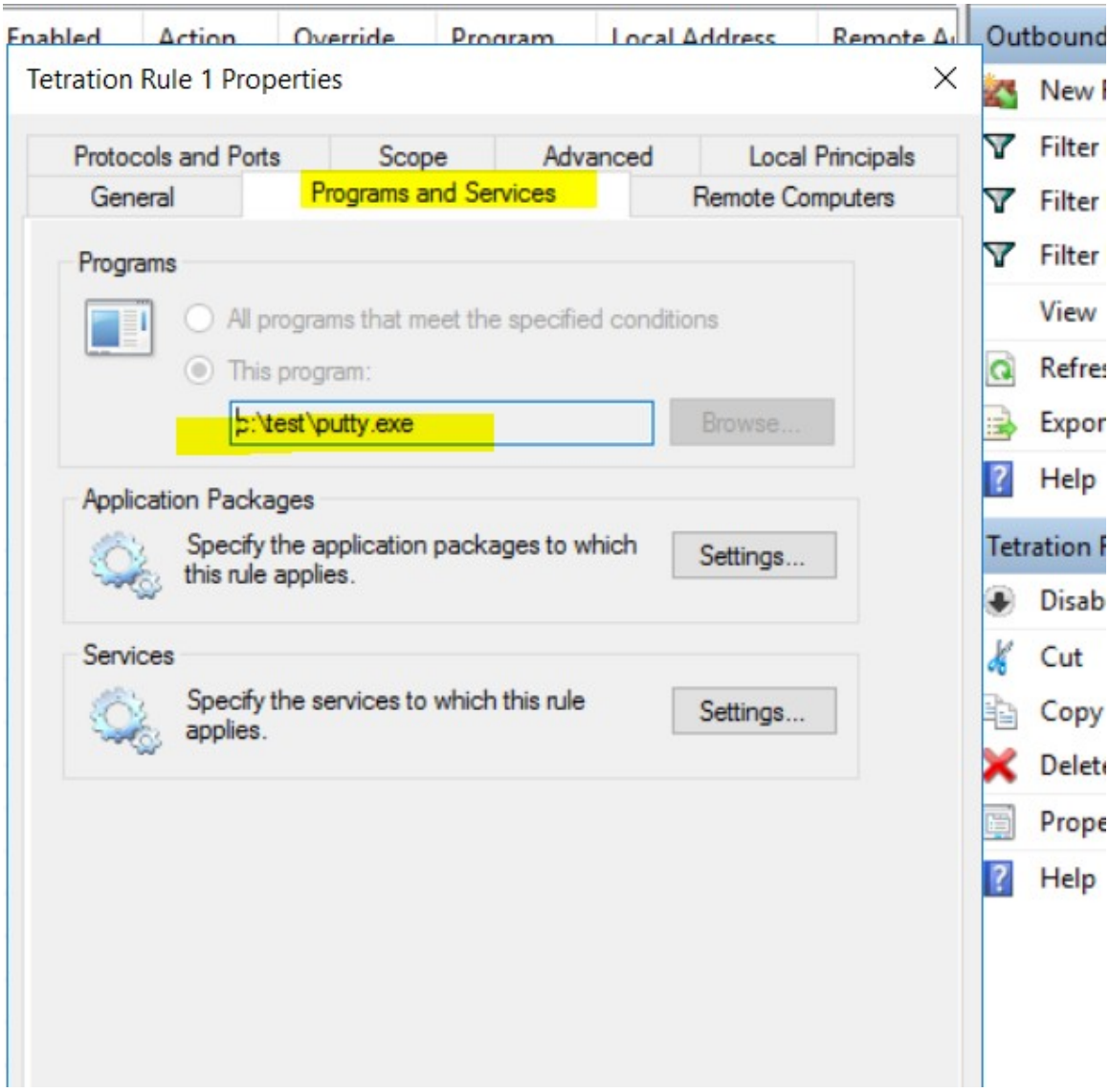
Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom de l'application sur les charges de travail avec système d'exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s'afficher sur la charge de travail pour un fichier binaire d'application saisi sous la forme **`c:\test\putty.exe`**.

Exemple de politique basée sur le nom de l'application

```
dst_ports {
start_port: 22
end_port: 22
consumer_filters {
application_name: "c:\test\putty.exe"
}
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier, à l'aide des outils Windows natifs, qu'un filtre a été ajouté à une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_APP_ID pour le nom de l'application dans le fichier de sortie : filter.xml.

```
<fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
```

```
                              <type>FWP_BYTE_BLOB_TYPE</type>
                              <byteBlob>
                                     <data>
‹→5c006400650076006900630065005c006800610072006400640069007300 6b0076006f006
‹→</data>
                                  <asString>\device\harddiskvolume2\temp\putty.exe</
‹→asString>
                 </byteBlob>
       </conditionValue>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:                    Cisco Secure Workload Rule 1
----------------------------------------------------
EffectiveWeight:                18446744073709551592
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    22
Protocol:                       6
AppID:                          \device\harddiskvolume2\test\putty.exe
```

Nom d'application non valide

- En mode WAF, une règle de pare-feu est créée pour un nom d’application non valide.
- En mode WFP, le filtre WFP n’est pas créé pour un nom d’application non valide, mais le NPC n’est pas rejeté. L'agent consigne un message d'avertissement et configure le reste des règles de politique.

Politiques basées sur le nom du service

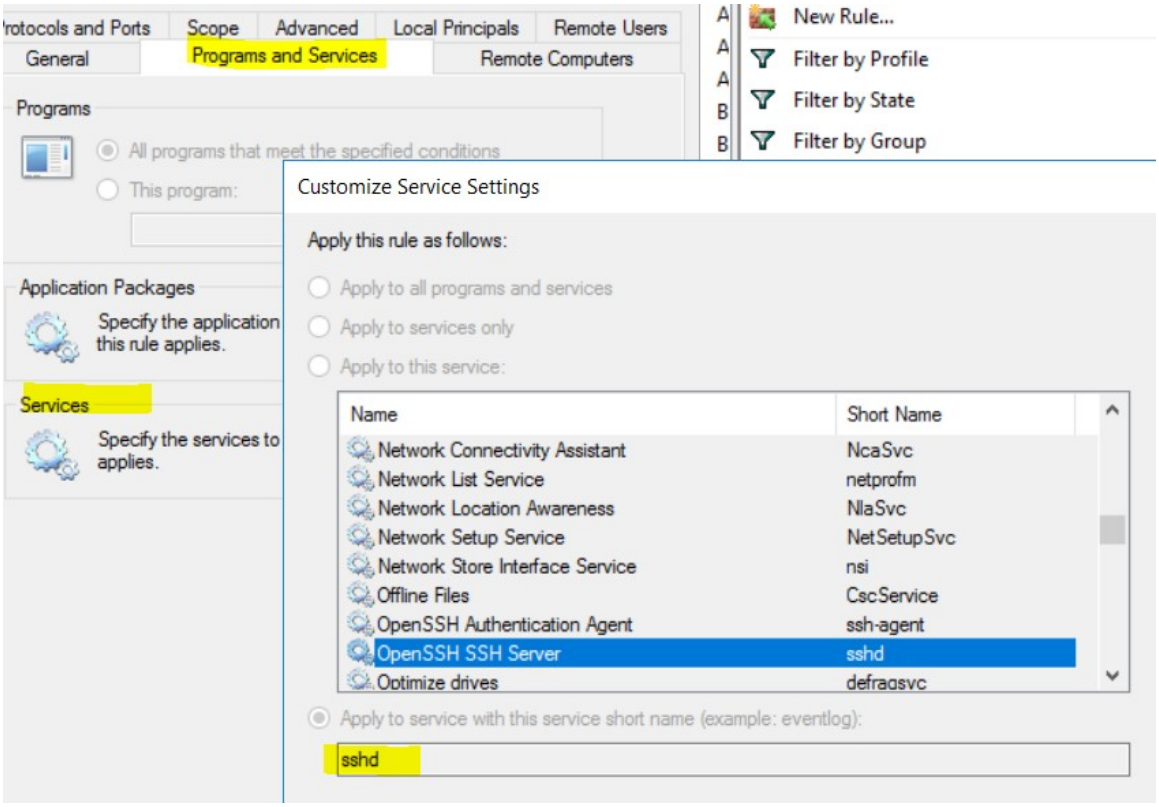
Utilisez les informations suivantes pour vérifier et dépanner les politiques basées sur le nom du service sur les charges de travail fonctionnant sous le système d’exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s’afficher sur la charge de travail.

Exemple de politique basée sur le nom de service

```
    dst_ports {
             start_port: 22
             end_port: 22
             provider_filters {
                    service_name: “sshd”
             }
         }}
         ip_protocol: TCP
         address_family: IPv4
         inspection_point: INGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
                    <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
                              <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>

<sd>O:SYG:SYD:(A;;CCRC;;;S-1-5-80-3847866527-469524349-687026318-
→516638107)</sd>
                    </conditionValue>
</item>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:       Cisco Secure Workload Rule 3
----------------------------------------------------
```

```
EffectiveWeight:            18446744073709551590
LayerKey:                   FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                     Permit
Local Port:                 22
Protocol:                   6
User or Service:            NT SERVICE\sshd
```

Nom non valide

- En mode WAF, la règle de pare-feu est créée pour un nom de service inexistant.
- En mode WFP, le filtre WFP n'est pas créé pour un nom de service inexistant.
- Le type de SID du service doit être *Unrestricted* (non restreint) ou *Restricted* (Restreint). Si le type de service est *None* (Aucun), la règle de pare-feu et le filtre WFP peuvent être ajoutés, mais n'ont aucun effet.

  Pour vérifier le type de SID, exécutez la commande suivante :

  ```
  sc qsidtype <service name>
  ```

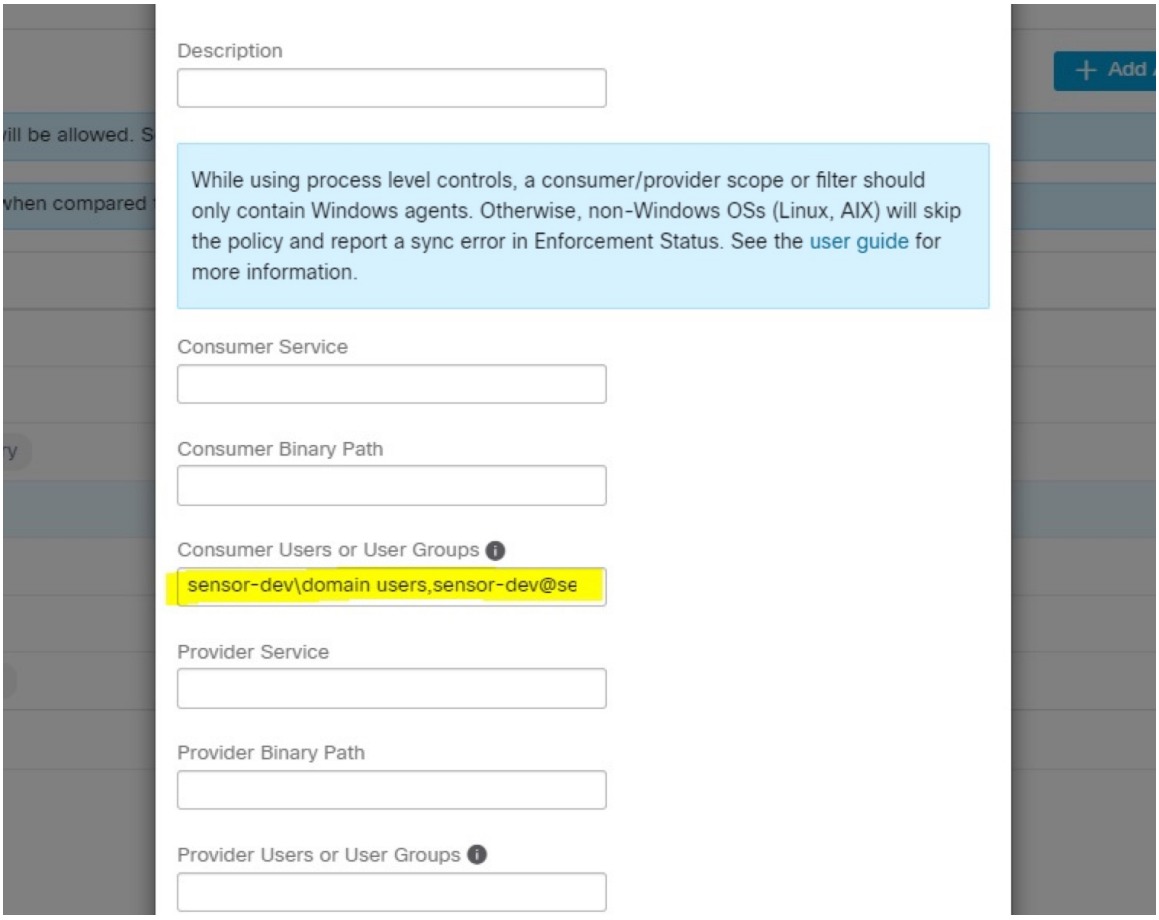
Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur

Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom d'utilisateur (avec et sans nom de groupe d'utilisateurs) sur les charges de travail avec système d'exploitation Windows.

Les sections de cette rubrique décrivent la manière dont les politiques doivent apparaître sur la charge de travail.

Les exemples présentés dans cette rubrique sont basés sur des politiques configurées avec les informations suivantes :

Figure 10: Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur



Exemple de politique basée sur le nom d'utilisateur

```
dst_ports {
          start_port: 30000
          end_port: 30000
          provider_filters {
               user_name: "sensor-dev\sensor-dev"
           }
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Exemple de politique basée sur le groupe d'utilisateurs et le nom d'utilisateur

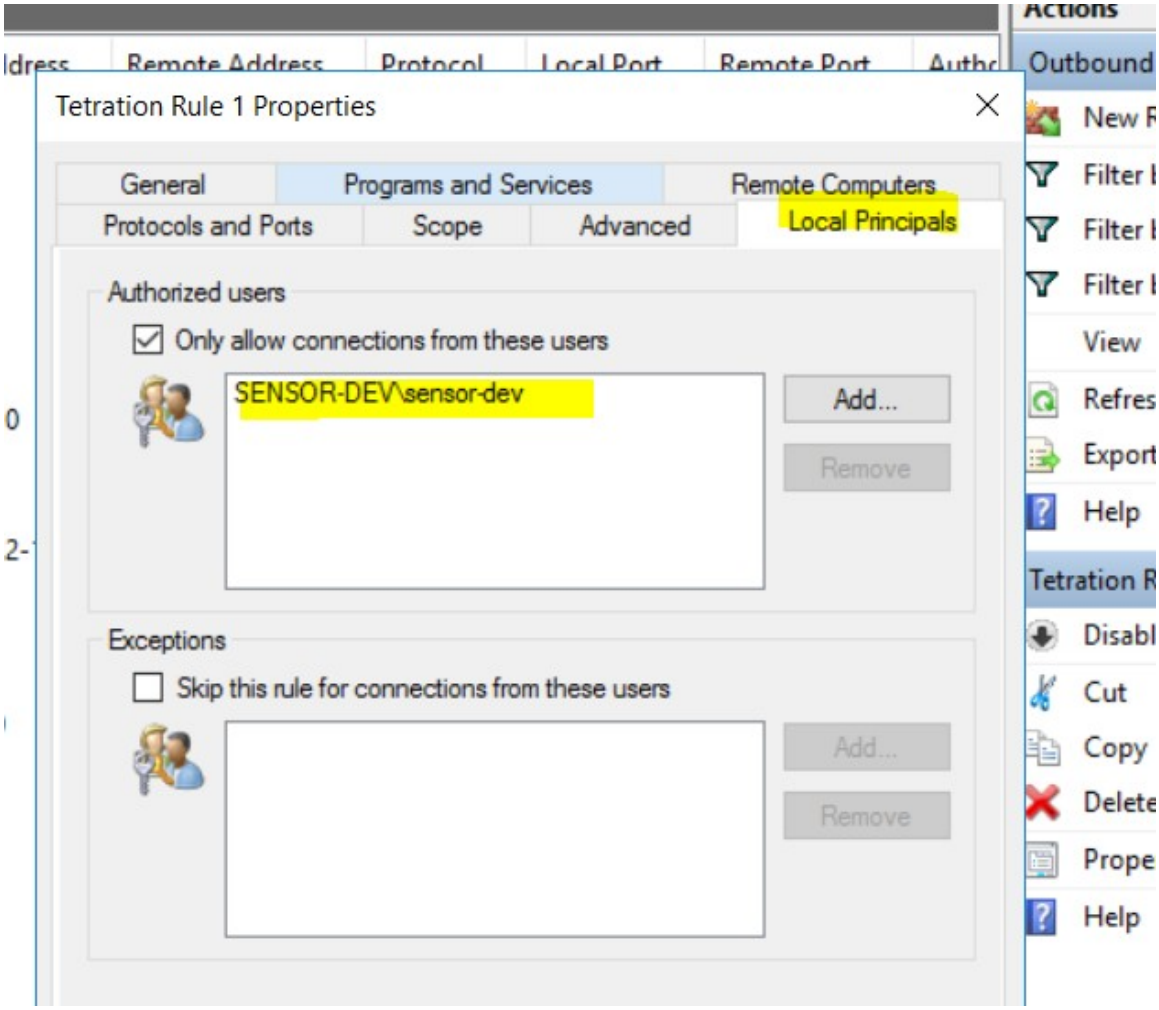
```
dst_ports {
start_port: 30000
end_port: 30000
provider_filters {
user_name: "sensor-dev\domain users,sensor-dev\sensor-dev"
}
}}
ip_protocol: TCP
```

```
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée

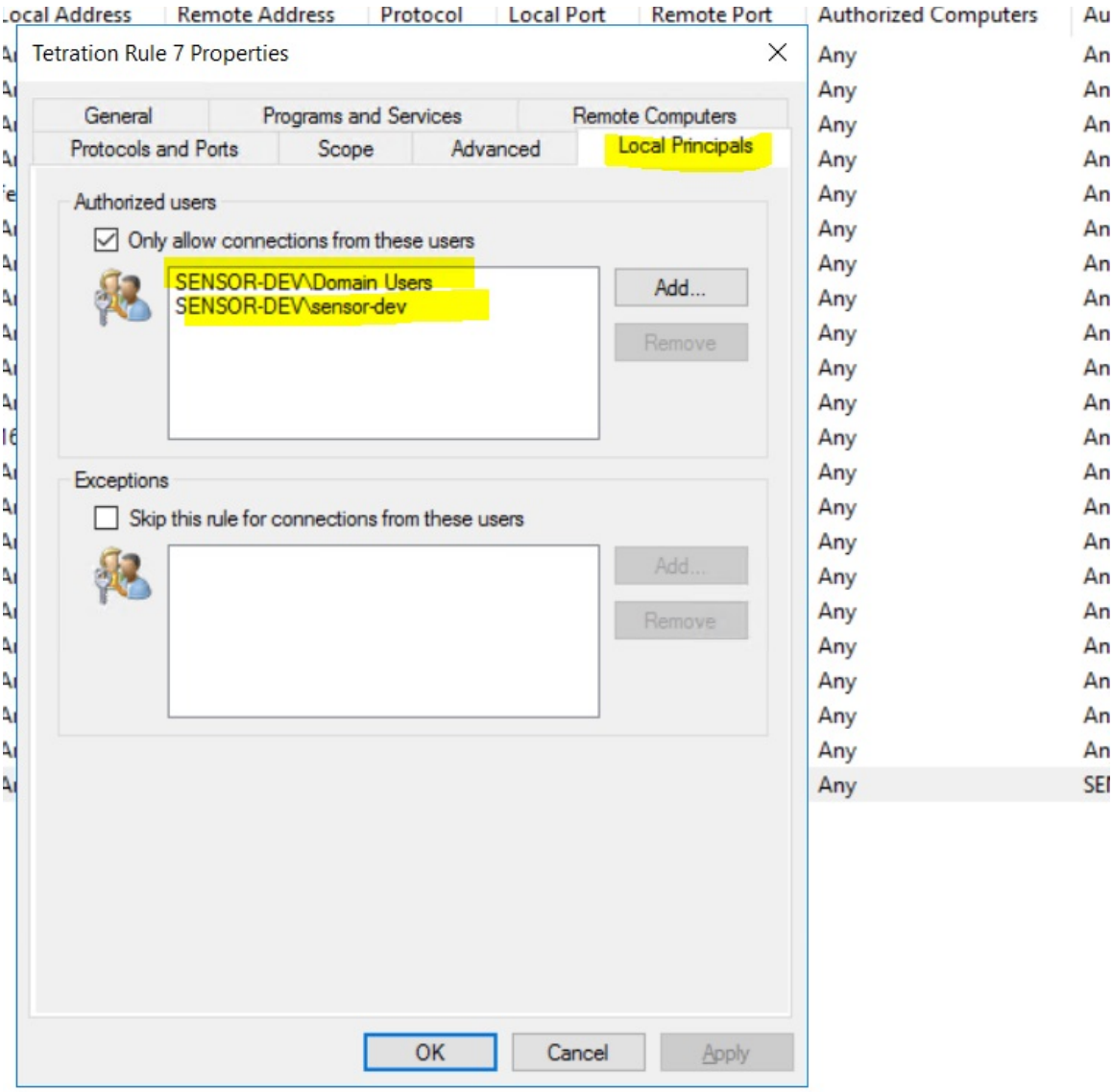
Règle de pare-feu basée sur le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\\sensor-dev



Règle de pare-feu basée sur le groupe d'utilisateurs et le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\sensor-dev et le groupe d'utilisateurs, domain users\sensor-dev



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
            <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
            <matchType>FWP_MATCH_EQUAL</matchType>
            <conditionValue>
```

```
                    <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>
                    <sd>O:LSD:(A;;CC;;;S-1-5-21-4172447896-825920244-2358685150)</sd>
                </conditionValue>
    </item>
```

Filtres WFP générés à l'aide de tetenf.exe -l -f

Filtrer en fonction du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\capteur-dev

```
Filter Name:                    Cisco Secure Workload Rule 1
-----------------------------------------------------------
EffectiveWeight:                18446744073709551590
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    30000
Protocol:                       6
User or Service:                SENSOR-DEV\sensor-dev
```

Filtrer en fonction du groupe d'utilisateurs et du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\\sensor-dev et le nom du groupe d'utilisateurs, SENSOR-DEV\\Domain Users

```
Filter Name:         Cisco Secure Workload Rule 1
-----------------------------------------------------
EffectiveWeight:             18446744073709551590
LayerKey:                    FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                      Permit
RemoteIP:                    10.195.210.15-10.195.210.15
Remote Port:                 30000
Protocol:                    6
User or Service:             SENSOR-DEV\Domain Users, SENSOR-DEV\sensor-dev
```

Le nom du service et le nom d'utilisateur ne peuvent pas être configurés dans le cadre d'une règle de politiques réseau.

Note La politique réseau est rejetée par l'agent Windows si le nom d'utilisateur ou le groupe d'utilisateurs n'est pas valide.

Application des Pods Kubernetes sur les nœuds Windows

Une fois que vous avez installé l'agent Kubernetes DaemonSet sur les nœuds de travail Windows, il capte les flux de réseau des nœuds de travail Windows et des pods Kubernetes dans un environnement AKS.

Exigences

- L'application des pods Kubernetes est prise en charge dans un environnement AKS avec des nœuds Windows.
- Le mode d'application DOIT être WFP avec l'option **Preserve Rules** (Règles conservées) désactivée.
- Pris en charge sur Microsoft Windows Server 2019 et Windows Server 2022.

Les politiques sont appliquées sur vSwitch pour les ports connectés aux pods à l'aide de VFP. La plateforme de filtrage virtuel (VFP) est un composant de vSwitch utilisé pour configurer des filtres pour le traitement du trafic réseau. Lors de l'application des politiques, le mode de conservation est désactivé.

Chaque filtre possède les attributs suivants :

- Id: Filter Name
- Direction : entrée ou sortie
- Type de règle : commutateur ou hôte.
  - Configurez le filtre sur vSwitch lorsque le type est Commutateur.
  - Créez un filtre WFP lorsque le type est Hôte.
- Action : Autoriser ou bloquer
- LocalPorts : il peut s'agir d'un port local ou d'une plage locale. Par exemple, 80 ou 100-200.
- RemotePorts : identique à LocalPorts, à distance.
- LocalAddresses : il s'agit d'une adresse ou d'une plage locale. Par exemple, 10.224.0.5, 10.224.1.0/24 (10.224.1.1-10.224.1.10 n'est pas autorisé).
- RemoteAddress : identique aux adresses locales, à distance.
- Protocole : ICMP/TCP/UDP/IGMP 255 est IPPROTO_RAW et 256 - PROTO_MAX

Les ports ne peuvent être spécifiés que pour UDP et TCP, et les ports ne sont pas autorisés dans la politique, sauf si un protocole est spécifié.

La configuration d'une politique sur un port virtuel est une opération basée sur la transaction. Si l'un des filtres n'est pas valide, l'application de l'ensemble de la politique échoue.

Il s'agit de l'application avec état. Les politiques basées sur les applications, les utilisateurs ou les services ne sont actuellement pas prises en charge.

Compatibilité avec Calico

L'application des pods fonctionne en mode « préserver les règles » désactivé. Lorsque l'agent Windows applique les règles aux pods, il supprime les politiques déjà configurées. Si le module d'extension Calico applique les politiques de réseau après l'agent, l'agent l'identifie comme un **écart**, et les politiques de réseau configurées par Calico sont supprimées et les politiques d'agent sont réappliquées.

Note Les politiques appliquées sont supprimées lorsque l'agent Windows est désinstallé sur les nœuds Windows.

Visibilité des filtres VFP configurés

L'option permettant de répertorier les filtres d'espaces à l'aide de Cisco Secure Workload n'est pas disponible. Dans un environnement AKS, vous pouvez utiliser le script PowerShell intégré. Exécutez le script PowerShell suivant : `c:\k\debug\collectlogs.ps1`. Affichez les fichiers de sortie **vfpoutput.txt** et **hnsdiag.txt** pour les filtres configurés.

Supprimer les filtres VFP configurés par l'agent Windows

1. Exécutez **cmd.exe** avec des privilèges d'administrateur.
2. Exécutez la commande : `<dossier d'installation>\tetenf.exe -d -f -pods -token=<yyyymm>`.

Note La commande supprime les filtres VFP pour tous les pods.

Dépannage des politiques appliquées et des flux réseau

1. Exécutez la commande suivante : `netsh wfp start capture keywords=19`.
2. Exécuter le trafic réseau
3. Cessez de capter les flux : `netsh wfp stop capture`.
4. Extrayez le fichier **wfpdiag.xml** du fichier **wfpdiag.cab**. Affichez les flux abandonnés.

Pour mapper les flux de réseau autorisés ou abandonnés aux politiques de pod :

1. Démarrez la session ETW : `logman start <nom de la session> -p Microsoft-Windows-Hyper-V-VfpExt -o <output file.etl> -ets`
2. Exécuter le trafic réseau
3. Arrêter la capture des flux : `stop logman`<nom de la session> .
4. Dans l'invite de commande, exécutez : `tracerpt <output file.etl>`. La commande crée le fichier **dumpfile.xml**. Affichez les flux du réseau.

Application des agents sur la plateforme AIX

Sur la plateforme AIX, l'agent Cisco Secure Workload utilise les utilitaires IPFilter pour appliquer les politiques de réseau. Par défaut, une fois l'agent activé sur l'hôte, il contrôle et programme le tableau de filtres IPv4. L'application de IPv6 n'est pas prise en charge.

IPFilter

Le paquet logiciel IPFilter sur AIX est utilisé pour fournir des services de pare-feu et est disponible sur AIX en tant que kit d'extension du noyau. Il se charge en tant que module d'extension de noyau, */usr/lib/drivers/ipf*. Il comprend les utilitaires ipf, ipPool, ipfstat, ipmon, ipfs et ipnat qui sont utilisés pour programmer les règles ipfilter. Chacun de ces règles spécifie les critères de correspondance d'un paquet. Pour en savoir plus, consultez les pages IPFilter dans le manuel AIX.

Lorsque l'application est activée, l'agent utilise IPFilter pour programmer le tableau de filtres IPv4 qui contient les règles d'autorisation ou d'abandon des paquets IPv4. L'agent regroupe ces règles pour classer et gérer les politiques à l'aide du contrôleur. Ces règles comprennent les règles Cisco Secure Workload dérivées des politiques et des règles générées par l'agent.

Lorsqu'un agent reçoit des règles indépendantes de la plateforme, il les analyse et les convertit en règles ipfilter ou ip pool et insère ces règles dans le tableau de filtrage. Après la programmation du pare-feu, l'agent d'application surveille le pare-feu pour détecter tout écart par rapport aux règles ou à la politique et, si c'est

le cas, reprogramme le pare-feu. L'agent effectue le suivi des politiques programmées dans le pare-feu et signale périodiquement leur état au contrôleur.

Une politique typique dans un message de politique de réseau indépendant de la plateforme se compose des éléments suivants :

```
source set id: "test-set-1"
destination set id: "test-set-2"
source ports: 20-30
destination ports: 40-50
ip protocol: TCP
action: ALLOW
...
set_id: "test-set-1"
   ip_addr: 1.2.0.0
   prefix_length: 16
   address_family: IPv4
set_id: "test-set-2"
   ip_addr: 5.6.0.0
   prefix_length: 16
   address_family: IPv4
```

Avec d'autres informations, l'agent traite la politique et la convertit en règles ippool et ipfilter spécifiques à la plateforme :

```
    table role = ipf type = tree number = 51400
    { 1.2.0.0/16; };

    table role = ipf type = tree number = 75966
    { 5.6.0.0/16; };

pass in quick proto tcp from pool/51400 port 20:30 to pool/75966 port 40:50 flags S/SA group
 TA_INPUT
pass out quick proto tcp from pool/75966 port 40:50 to pool/51400 port 20:30 flags A/A group
 TA_OUTPUT
```

Mises en garde

Sauvegarde du pare-feu de l'hôte

Lorsque la mise en application est activée pour la première fois dans un profil de configuration d'agent, les agents exécutés sur les hôtes AIX, avant de prendre le contrôle du pare-feu de l'hôte, stockent le contenu actuel des fichiers ippool et ipfilter dans */opt/cisco/tetration/backup*. Les transitions successives pour activer ou désactiver la configuration d'application ne génèrent pas de sauvegardes. Le répertoire n'est pas supprimé lors de la désinstallation de l'agent.

Limites connues

L'application de IPv6 n'est pas prise en charge.

État et statistiques de l'agent

Procedure

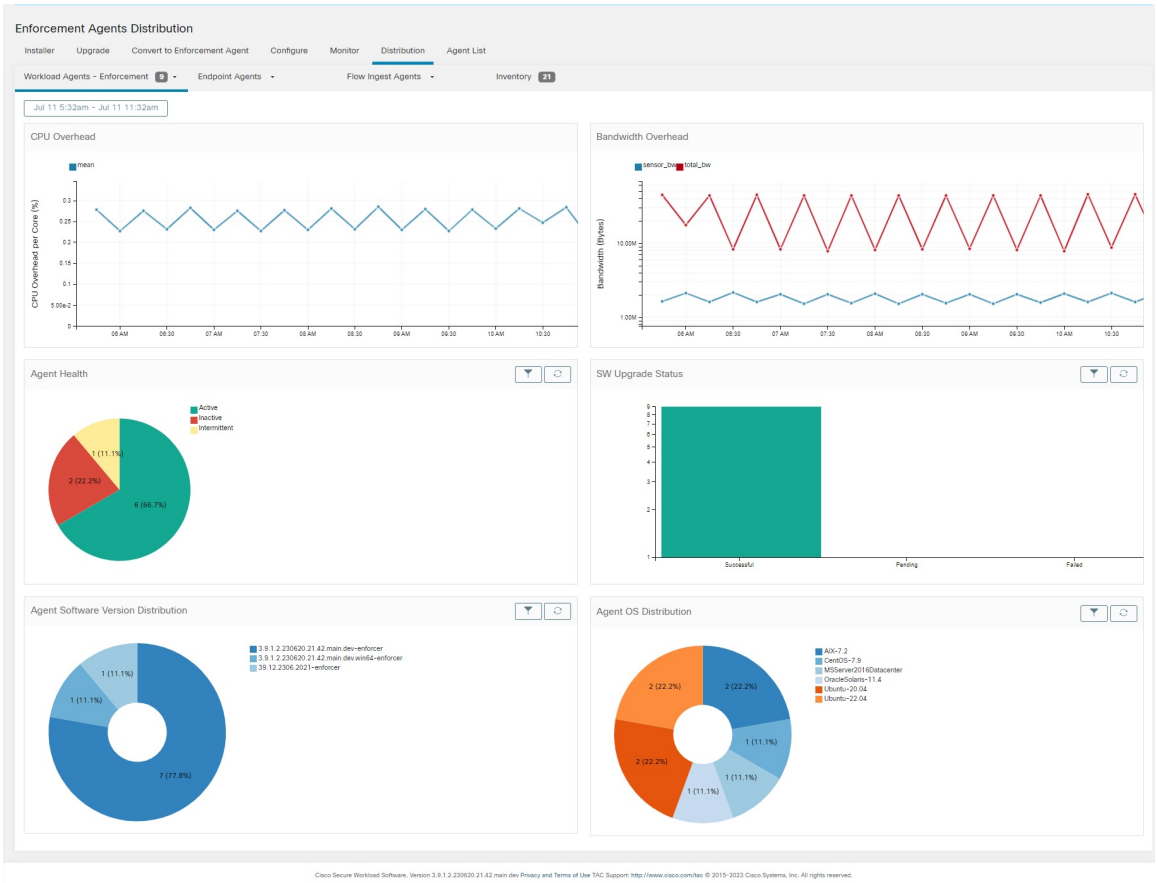
Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)**.

Étape 2 Cliquez sur l'onglet **Distribution** (Répartition).

Étape 3 Cliquez sur un type d'agent en haut de la page.

Étape 4 Sur cette page, vous pouvez vérifier la surcharge du CPU, la surcharge de la bande passante, l'intégrité de l'agent, l'état des mises à jour logicielles, la répartition des versions du logiciel de l'agent et la répartition du système d'exploitation de l'agent.

Figure 11: Page Répartition des agents



Note **Intégrité de l'agent** : l'agent effectue une vérification périodique toutes les 10 à 30 minutes. S'il n'y a aucun enregistrement pendant plus d'une heure trente, l'agent est inactif. Pour réduire les fausses alertes, l'état d'intégrité de l'agent est défini à intermittent au lieu d'inactif si l'intervalle d'enregistrement est compris entre 1 heure et 1 heure 30.

Pour en savoir plus sur l'état de l'application, consultez la section État de l'application.

Afficher les détails de l'agent

Les étapes suivantes fournissent l'une des options disponibles pour accéder à la page Workload Profile (Profil de la charge de travail), qui affiche des détails sur la charge de travail et son agent installé.

Procedure

Étape 1 Dans le menu de navigation, cliquez sur**Organize** > > **Scopes and Inventory** (Organiser > Portées et inventaire).

Étape 2 Recherchez une charge de travail pour laquelle vous souhaitez afficher les détails.

Étape 3 Cliquez sur l'adresse IP pour afficher des détails tels que l'intégrité de l'agent, l'adresse IP, la portée, le type d'inventaire, les groupes d'application, les groupes expérimentaux, les étiquettes d'utilisateur et le volume de trafic (total des octets/total des paquets).

Pour en savoir plus, consultez Profil de la charge de travail, on page 401.

Configuration de l'agent logiciel

Exigences et conditions préalables à la configuration des agents logiciels

- Assurez-vous de disposer des informations d'authentification pour le rôle d'utilisateur Cisco Secure Workload requises :
  - Administrateur de site
  - Le service d'assistance à la clientèle

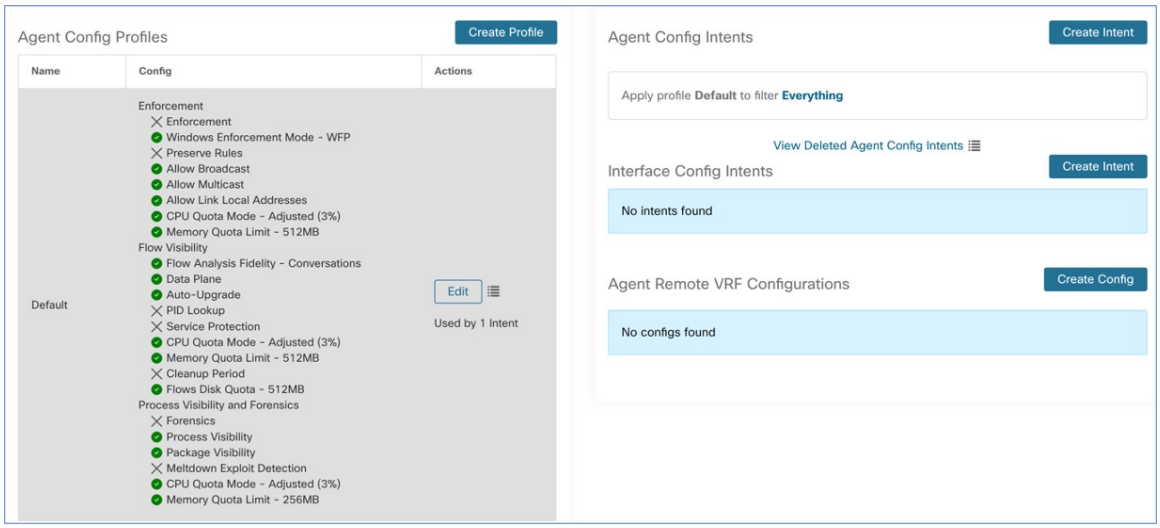
  Pour en savoir plus, consultez Rôles des utilisateurs et accès à la configuration des agents, on page 80.
- Assurez-vous de disposer des privilèges sur l'hôte pour exécuter le service d'agent sur chaque charge de travail. Pour en savoir plus, consultez la section Gestion des services des agents.
- Vérifier les plateformes prises en charge, la configuration requise et les instructions d'installation pour les agents. Pour en savoir plus, consultez la section Déployer des agents logiciels.

Rôles des utilisateurs et accès à la configuration des agents

1. Les propriétaires de la portée racine ont accès uniquement pour créer un profil de configuration et une spécification d'intent de configuration.
2. En tant que propriétaire d'une portée racine, vous pouvez créer des profils de configuration qui sont associés uniquement aux portées détenues et imposer ces profils de configuration aux agents.

Note Sous le profil de configuration de l'agent, vous pouvez maintenant afficher le nombre d'intents utilisant le profil de configuration avant de modifier le profil.

Figure 12: Configuration d'agent logiciel pour les propriétaires de portée



3. Les administrateurs du site ont accès à tous les composants de la page de Agent Configuration (configuration de l'agent), qui comprend la spécification des intents de configuration de l'interface et les configurations de Routage et transferts virtuels.

Configurer les agents logiciels

Sur la page de configuration de l'agent logiciel (Software Agent Configuration), configurez les agents logiciels pour créer des intents qui sont associés à un **filtre d'inventaire** ou à une **portée**. Pour chaque agent, appliquer le premier intent correspondant. Pour en savoir plus, consultez Inventory, on page 349.

Note Pour tout déploiement, Cisco Secure Workload, utilisez la configuration d'agent par défaut sur tous les agents qui ne sont associés à aucun profil de configuration spécifique.

Figure 13: Configuration de l'agent logiciel

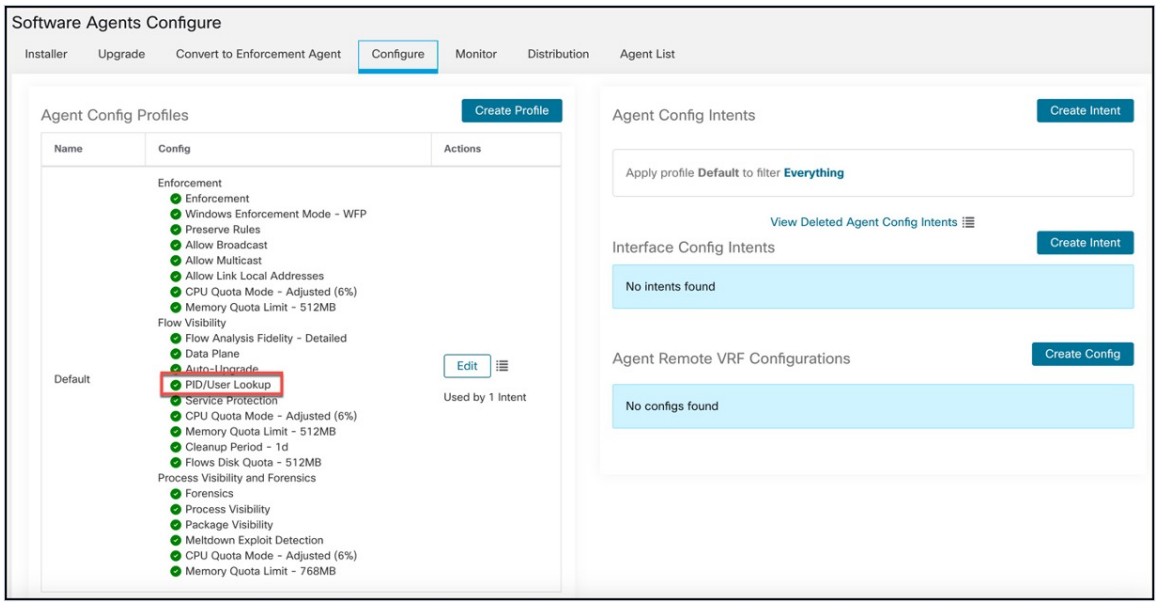
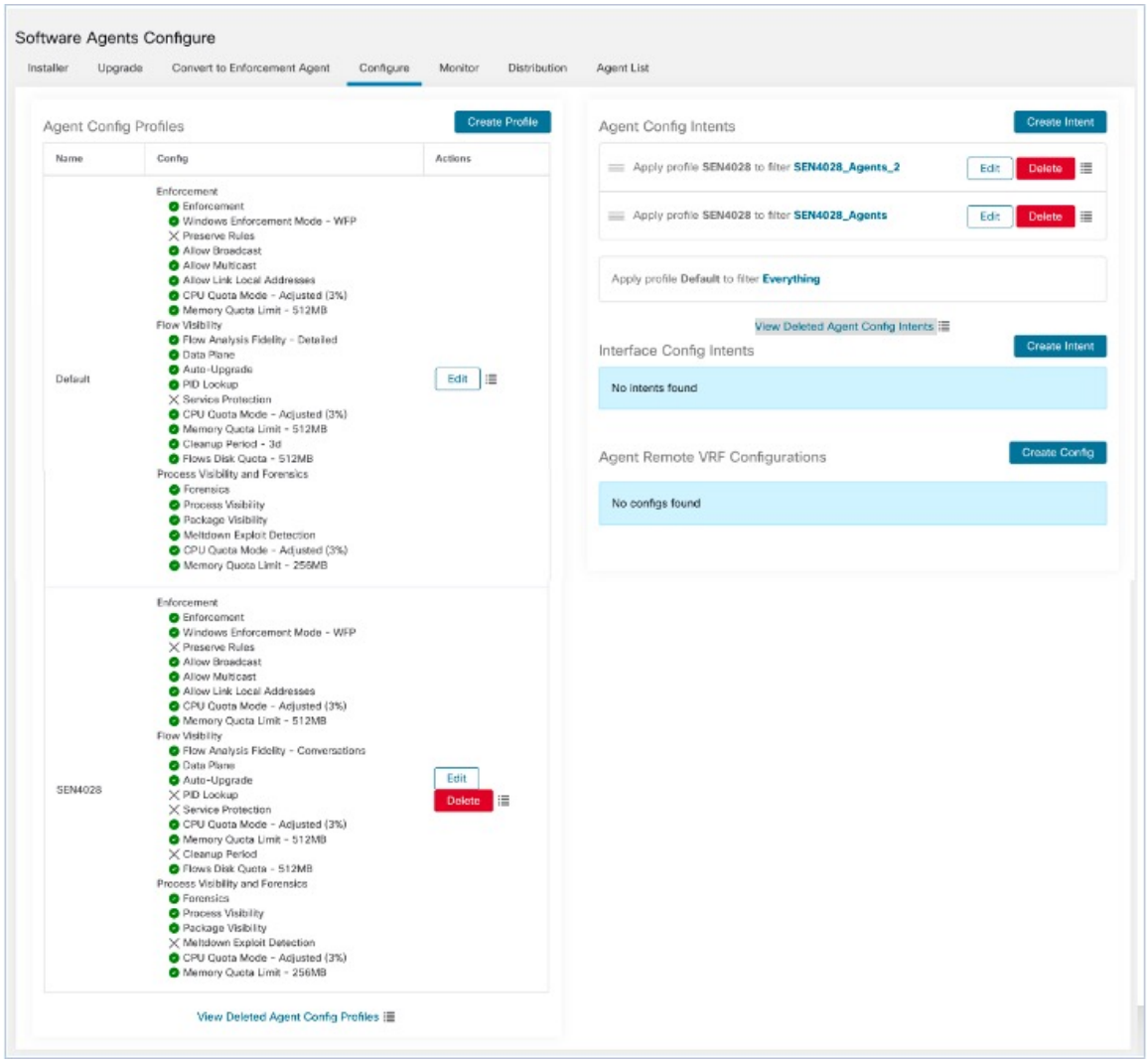


Figure 14: Configuration de l'agent logiciel



Creating an Agent Config Profile

Before you begin

See Exigences et conditions préalables à la configuration des agents logiciels, on page 80.

Procedure

Étape 1 In the navigation bar on the left, click **Manage** > **Agents**.

Étape 2 Click the **Configure** tab.

Étape 3 Click the **Create Profile** button.

Étape 4 Enter a name for the profile (required) and select a scope where profile will be available.

Étape 5 Enter the appropriate values in the fields listed in the tables below:

Table 11: Enforcement config

Option	Description
Enforcement	**Enable** - Enable policy enforcement on the agent. Soon after you enable enforcement, the agent enforces the most recently received policy set, if any. **Disable** (Default) - The agent will not enforce policy. **Note** If enforcement is enabled, and you disable and then re-enable enforcement, the firewall state is cleared and the catch-all default action is set to ALLOW.
Preserve Rules	**Enable** - Preserves any existing firewall rules on agent. **Disable** (Default) - Clears existing firewall rules before applying enforcement policy rules from Cisco Secure Workload. Behavior depends on the platform. To see specifics for each platform, search this document for "preserve rules"
Allow Broadcast	**Enable** (Default) - Adds rules to the firewall to allow ingress and egress broadcast traffic on the workload. **Disable** - Does not add any rule. Broadcast traffic will be dropped if default policy is deny on Agent.
Allow Multicast	**Enable** (Default) - Adds rules to the firewall to allow ingress and egress multicast traffic on the workload. **Disable** - Does not add any rule. Multicast traffic will be dropped if default policy is deny on Agent.
Allow Link Local	**Enable** (Default) - Adds rules to the firewall to allow link local addresses' traffic on the workload. **Disable** - Does not add any rule. Multicast traffic will be dropped if default policy is deny on Agent.
CPU Quota Mode for enforcement process	**Adjusted** (Default) - The CPU limit is adjusted according to the number of CPUs on the system. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system, selecting this mode means that agent is allowed to use a total of 30% (measured by top). **Top** - The CPU limit value would match the top view on average. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system. The CPU usage would still be 3%. This is a fairly restrictive mode and should be used only when necessary. **Disable** - The CPU limit feature is disabled. The agent will use CPU resources permitted by the OS. See agent_cpu_sla.pdf for more information.
CPU Quota Limit (%)	Specify the actual limit in percentage of the system processing power the agent can use.

Option	Description
Memory Quota Limit (MB)	Specify the memory limit in MB that the process is allowed to use. If the process hits this limit, it will restart.
Windows Enforcement Mode	On Windows workloads, agents can enforce network policies using: • **WFP** - Windows Filtering Platform (by directly programming WFP filters in the Windows Filter Engine.) See Mise en application par les agents sur la plateforme Windows en mode WFP, on page 60. • **WAF** (Default) - Windows Advanced Firewall. See Application par les agents sur la plateforme Windows en mode WAF, on page 57.

Table 12: Flow Visibility config

Field	Description
Flow Analysis Fidelity	**Conversations** - Enable conversations mode on all sensors. **Detailed** (Default) - Enable detailed mode on all sensors .
Data Plane	**Enable** (Default) - Enable the agent to send reports to the cluster. **Disable** - Disable the agent's reports.
Auto-Upgrade	**Enable** (Default) - Automatically upgrade the agent when a new package is available. **Disable** - Do not automatically upgrade the agent.
PID Lookup	**Enable** - Enable PID lookups on the agent. When enabled, the agent will make best-effort attempts to associate network flows with running processes in the workload. This operation might be expensive, therefore the agent will throttle the number of operations done in each export cycle to keep the CPU overhead under control. It is possible that some flows are not associated with any processes even when the config is enabled. **Disable** (Default) - Do not enable PID lookups on the agent.

Field	Description
Service Protection	**Enable** - Enable service protection on the agent. When enabled, the agent ensures it prevents users from disabling the service, from uninstalling the agent, and from restarting the service. However, once the service protection is disabled, users can continue to stop or uninstall the agent. **Note** • Do not disable service protection for normal auto upgrade of an agent. • Do not enable service protection for manual upgrade of an agent. • Service protection blocks any forced upgrades, such as using the installer script - forceUpgrade option. • Any system initiated upgrade works seamlessly when the service protection is enabled. **Disable(*)**-By default, service protection is disabled on the agent. **Detailed** (Default) - Enable detailed mode on all sensors. **Note** This feature is available only for Windows agent.
CPU Quota Mode	**Adjusted** (Default) - The CPU limit is adjusted according to the number of CPUs on the system. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system, selecting this mode means that agent is allowed to use a total of 30% (measured by top). **Top**- The CPU limit value would match the top view on average. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system. The cpu usuage would still be 3%. This is a fairly restrictive mode and should be used only when necessary. **Disable** - The CPU limit feature is disabled. The agent will use CPU resources permitted by the OS. See agent_cpu_sla.pdf for more information.
CPU Quota Limit (%)	Specify the actual limit in percentage of the system processing power the agent can use.
Memory Quota Limit (MB)	Specify the memory limit in MB that the process is allowed to use. If the process hits this limit, it will restart.
Cleanup period (days)	**Enable** - Enable automated cleanup on the agent. Enter the number of days after which the inactive agent is removed. **Disable** (Default) - Do not enable automated cleanup on the agent.
Flow Analysis Fidelity	**Conversations** - Enable conversations mode on all sensors. **Detailed** (Default) - Enable detailed mode on all sensors
Flows Disk Quota (MB)	Specify in MB the total size limit of stored flow data.

Field	Description
Flows Time Window (h)	Specify in hours how long the agent must capture and store flows locally. You may either select **Flows Disk Quota** or **Flows Time Window**; it's either size-based or time-based rotation. On selecting Flows Time Window, the Flows Disk Quota is set to 16GB. Setting Flows Disk Quota to 0 disables this feature. The flow data is rotated once it reaches either size limit or time limit.

Figure 15: Flow Visibility

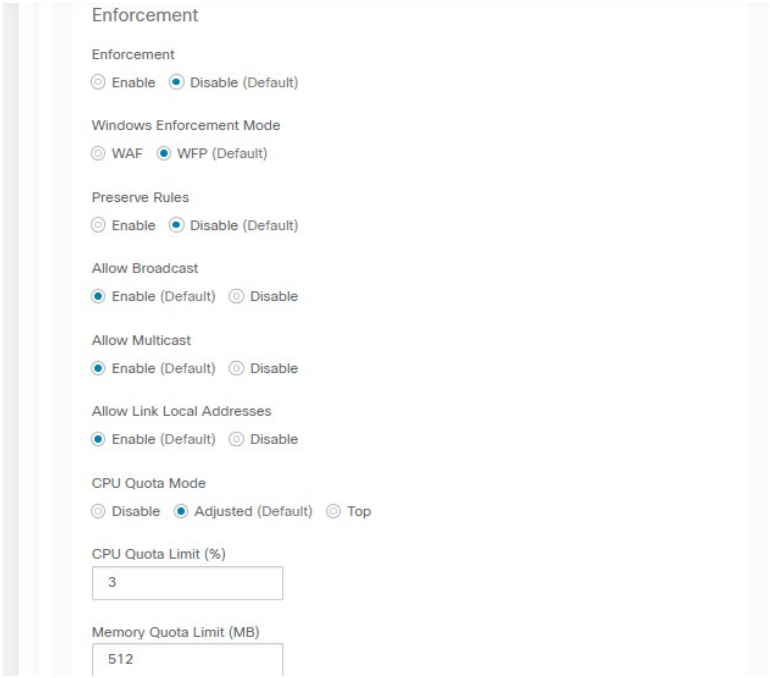


Figure 16:

Table 13: Process Visibility and Forensics Config

Field	Description
Forensics	**Enable** - Enable forensics on the agent. Note that this feature may consume additional CPU cycles specified in the CPU limit below. For example, if the cpu limit is 3% and this feature is enabled, the agent assumes it could use up to 6% in total. **Disable** (Default) - Disable forensics on the agent.
Meltdown Exploit Detection	**Enable** - Enable Meltdown exploit detection on the agent. This feature requires Forensics to be enabled. For more information, see Side Channel in the Compatibilité, on page 598. **Disable** (Default) - Disable Meltdown exploit detection on the agent
CPU Quota Mode	**Adjusted** (Default) - The CPU limit is adjusted according to the number of CPUs on the system. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system, selecting this mode means that agent is allowed to use a total of 30% (measured by **top**). **Top** - The CPU limit value would match the top view on average. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system. The cpu usuage would still be 3%. This is a fairly restrictive mode and should be used only when necessary. **Disable** - The CPU limit feature is disabled. The agent will use CPU resources permitted by the OS.
CPU Quota Limit (%)	Specify the actual limit in percentage of the system processing power the agent can use.
Memory Quota Limit (MB)	Specify the memory limit in MB that the process is allowed to use. If the process hits this limit, it will restart.

Étape 6 Click **Save**

What to do next

Associate this profile with an agent config intent. See Création d'un intent de configuration d'agent, on page 90.

Création d'un intent de configuration d'agent

Before you begin

- Consultez Exigences et conditions préalables à la configuration des agents logiciels, on page 80.
- Créez un profil de configuration d'agent. Consultez Creating an Agent Config Profile, on page 83.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **Agents (Agents)**.

Étape 2 Cliquez sur l'onglet**Configure** (Configurer).

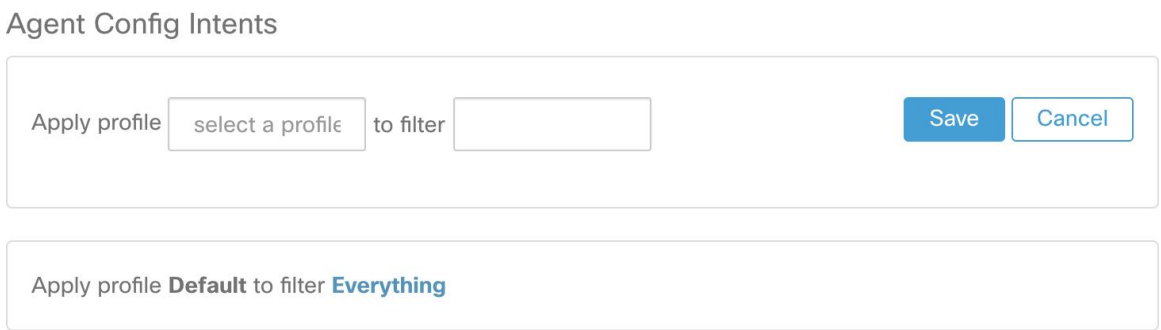
Étape 3 Cliquez sur le bouton **Create Intent** (créer un intent) à côté de l'en-tête de **l'intent de configuration de l'agent**.

Étape 4 Saisissez les valeurs appropriées dans les champs répertoriés dans le tableau ci-dessous :

Champ	Description
Profil (obligatoire)	Saisissez le nom d'un profil existant et sélectionnez-le dans le menu déroulant.
Filtre (obligatoire)	Saisissez le nom d'un filtre existant ou de la portée, ou sélectionnez *Create new filter* (créer un filtre) dans le menu déroulant. Consultez la section Filtres pour en savoir plus sur la création de filtres.

Étape 5 Cliquez sur **Save** (enregistrer).

Figure 17: Intents de configuration de l'agent



Création d'une configuration VRF distante pour les agents

C’est la méthode recommandée pour affecter les VRF aux agents logiciels Cisco Secure Workload. À l’aide de cette configuration, le dispositif Cisco Secure Workload affecte des VRF aux capteurs logiciels en fonction de l’adresse IP source et du port source vus pour ces agents sur les connexions à l’appareil Cisco Secure Workload.

Procedure

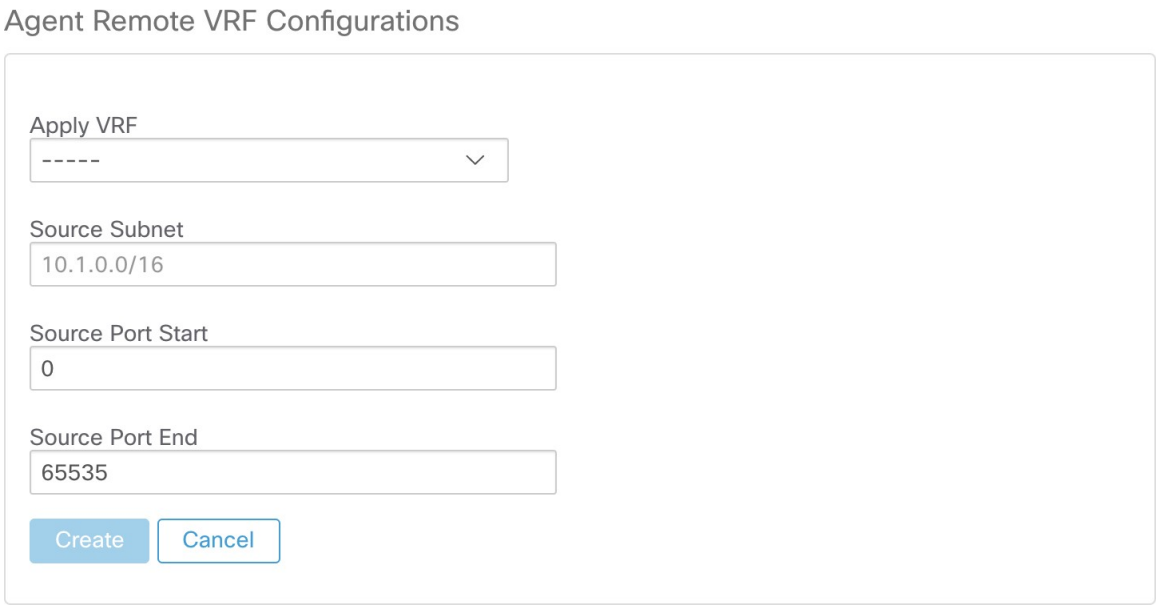
Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **Agents (Agents)**.

Étape 2 Cliquez sur l’onglet**Configure** (Configurer).

Étape 3 Cliquez sur le bouton **Create Config** (créer une configuration) à côté de l’en-tête **Agent Remote VRF Configurations** (Configurations VRF à distance de l'agent).

Étape 4 Saisissez les valeurs appropriées dans les champs et cliquez sur **Save** (Enregistrer).

Figure 18: Configuration VRF à distance



Créer un intent de configuration d’interface

Nous vous recommandons d’affecter le routage et le transfert virtuels (VRF) aux agents dans les paramètres de configuration d’un VRF distant. Dans de rares cas, lorsque les hôtes d’agent ont plusieurs interfaces qui doivent être affectées à différents VRF, vous pouvez choisir de leur affecter des VRF à l’aide des intents de configuration d’interface.

Procedure

Étape 1 Accédez à **Manage (Gestion)** > **Agents**.

Étape 2 Cliquez sur l'ongletConfigure (Configurer).

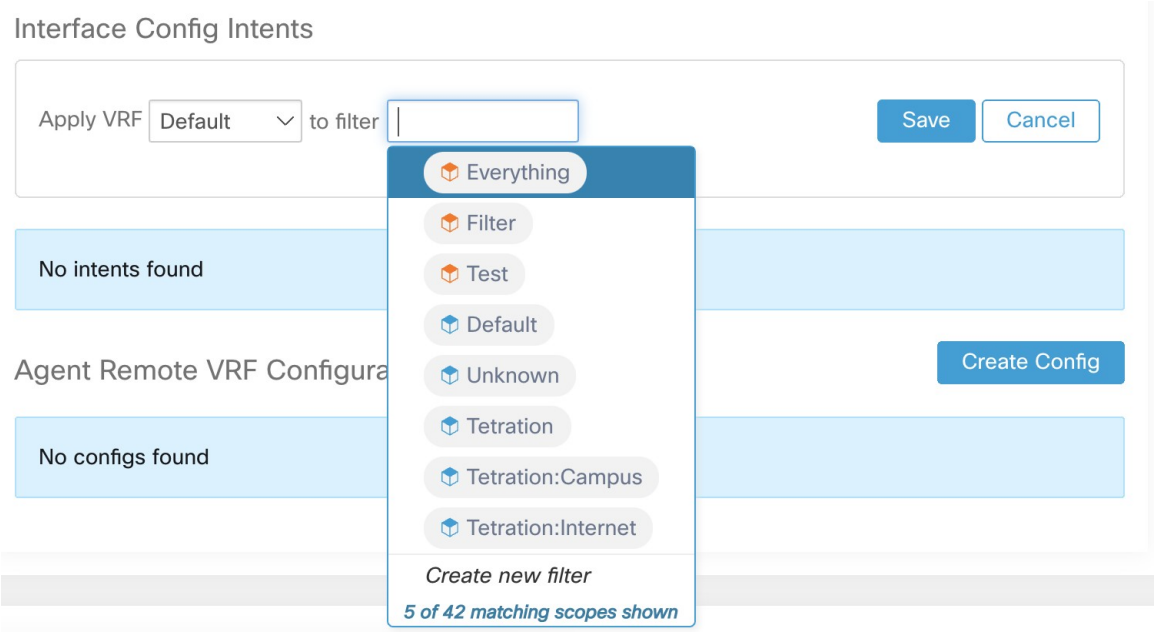
Étape 3 Cliquez sur le bouton **Create Intent** (Créer un intent) à côté de l'en-tête **Interface Config Intent** (Intent de configuration d'interface).

Étape 4 Saisissez les valeurs appropriées dans les champs répertoriés dans le tableau :

Champ	Description
VRF	Choisissez un VRF dans la liste déroulante (obligatoire).
Filter (Filtrer)	Saisissez le nom d'un filtre existant ou d'une portée, ou sélectionnez *Create a new filter* (créer un filtre) dans la liste déroulante (obligatoire). Pour en savoir plus, consultez Filtres.

Étape 5 Cliquez sur **Save** (enregistrer).

Figure 19: Intents de configuration d'interface



Note Lorsque vous supprimez une interface avec un intent de configuration de priorité plus élevée, les agents ne passent pas à l'intent collecteur par défaut.

Afficher l'état détaillé de l'agent dans le profil de charge de travail

Procedure

Étape 1 Suivez les étapes ci-dessus pour vérifier l'état de l'agent.

Étape 2 Dans la page Enforcement Agents (Agents d'application), cliquez sur **Agent OS Distribution**(Répartition des agents par SE). Sélectionnez un système d'exploitation et cliquez sur l'image du filtre dans le coin supérieur droit de la zone.

Étape 3 Sur la page Software Agent List (Liste des agents logiciels), les agents sont répertoriés avec la distribution sélectionnée du système d'exploitation.

Étape 4 Cliquez sur **Agent** (agent) pour obtenir les détails de l'agent, puis cliquez sur IP address (adresse IP). Dans la page Workload Profile (profil de charge de travail), vous pouvez afficher les détails du profil d'hôte, du profil d'agent et des détails propres à l'agent, comme la bande passante, les processus de longue durée, les paquets, l'instantané du processus, la configuration, les interfaces, les statistiques, les politiques, les politiques de conteneur, etc.

Étape 5 Cliquez sur l' **onglet Config** pour voir la configuration sur l'hôte final.

Étape 6 Cliquez sur l' **onglet Policies** (Politiques) pour voir les politiques appliquées sur l'hôte final.

Figure 20: Profil de la charge de travail - Config

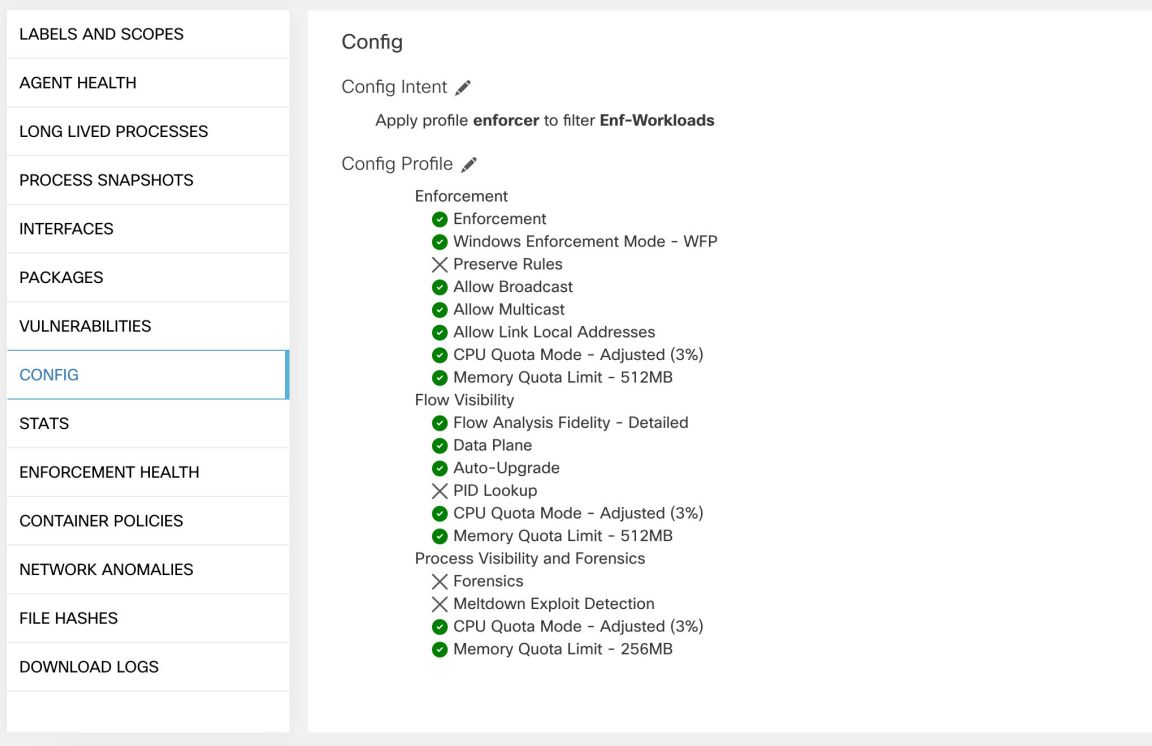
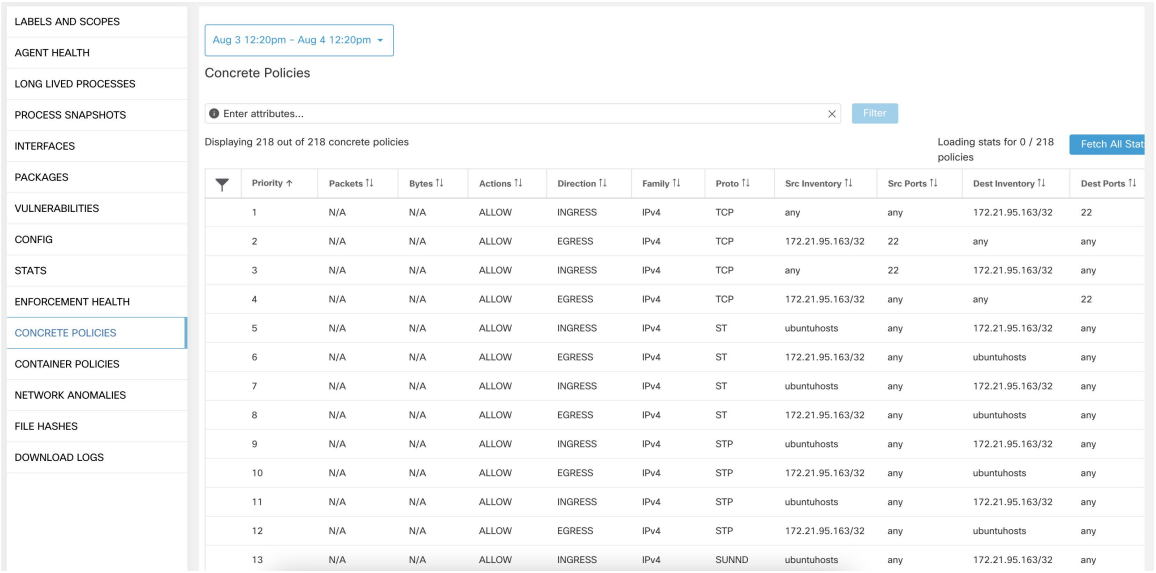


Figure 21: Profil de la charge de travail - Politiques



Note **Fetch All Stats (La récupération de toutes les statistiques)** n'est pas prise en charge sur les hôtes d'agent Windows, qui sont utilisés pour fournir des statistiques pour les politiques individuelles.

Relocalisation des agents

La relocalisation des agents est la méthode pour déplacer les utilisateurs sur site vers le logiciel-service ou du logiciel-service vers l'environnement sur site.

Rôles utilisateur

- Administrateur de site
- Représentant du service d'assistance à la clientèle

Vous pouvez migrer vers ou depuis un environnement de logiciel-service, en particulier, lorsque vous passez d'un logiciel-service à un environnement sur site, vous devez travailler avec une équipe de soutien interne.

Flux de travaux

- Saisissez la clé d'activation, l'adresse IP virtuelle du capteur et l'autorité de certification du capteur (AC), puis Activer la relocalisation, on page 95.
- Sélectionner les agents à relocaliser, on page 96.
- Désactiver la relocalisation, on page 97.

Note À tout moment, vous ne pouvez déplacer un agent que vers une seule destination. Nous vous recommandons de désactiver la relocalisation de l'agent après avoir déplacé l'agent.

Activer la relocalisation

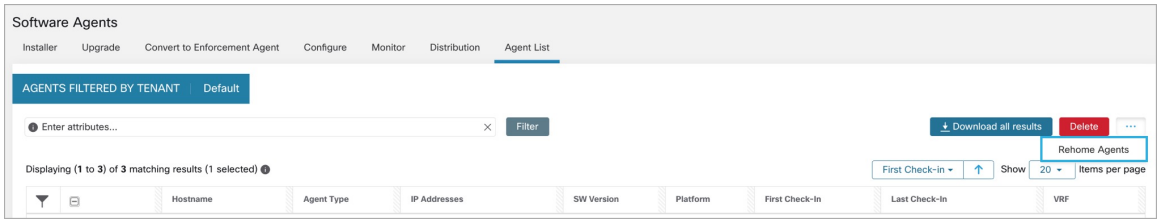
Procedure

Étape 1 Dans le volet de navigation, cliquez sur **Manage(Gestion)**>**Workloads (Charges de travail)**> **Agents (Agents)**.

Étape 2 Cliquez sur l'onglet **Agent List** (liste des agents).

Étape 3 Cliquez sur l'icône de menu et sélectionnez **Rehome Agents** (Relocaliser les agents).

Figure 22: Agents relocalisés

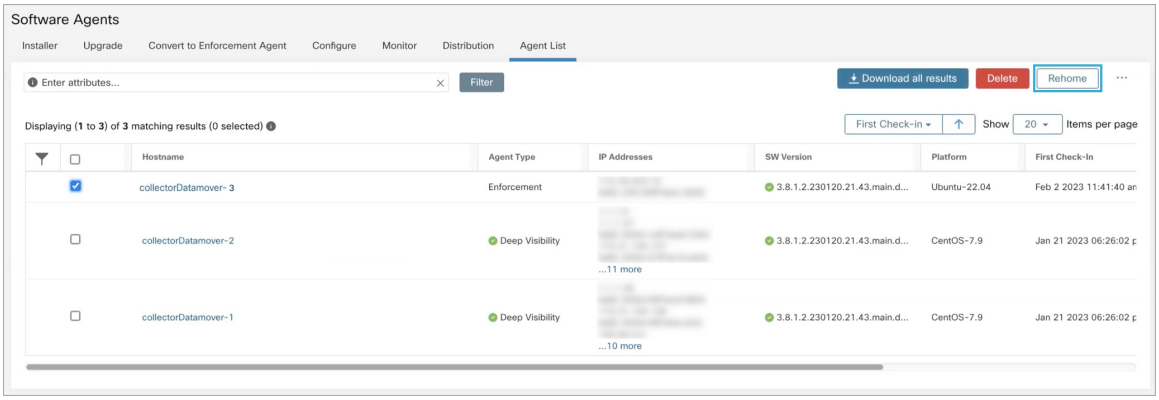


Étape 4 Dans la fenêtre **Agent Rehoming**(Relocalisation des agents), saisissez les détails suivants :

Champ	Description
Clé d'activation de la portée de la destination	**a.** Accédez à **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)**. **b.** Cliquez sur l'onglet **Installer** (Programme d' installation). **c.** Sélectionnez **Manual install using classic packaged installers (Installation manuelle à l'aide des programmes d'installation classiques).** **d.** Cliquez sur **Next** (suivant). **e.** Cliquez sur **Agent Activation Key** (clé d'activation de l'agent). **f.** Copiez la valeur de la **clé** et collez-la dans le champ **Destination Scope Activation Key** (Clé d'activation de la portée de destination).

Champ	Description
VIP de capteur de destination	**a.** Naviguez jusqu'à **Platforms**(Plateforme) > **Cluster Configuration** (configuration de la grappe). **b.** Copiez la **VIP de capteur** et collez-la dans le champ **Destination Sensor VIP** (VIP de capteur de destination).
Serveur mandataire HTTPS	Saisissez un domaine ou une adresse de serveur mandataire en fonction des besoins de l'agent pour utiliser un serveur mandataire pour la communication sortante.
Certificat d'autorité de certification du capteur de destination	**a.** Naviguez jusqu'à **Platforms**(Plateforme) > **Cluster Configuration** (configuration de la grappe). **b.** Cliquez sur **Download Sensor CA Cert** (Télécharger le certificat de l'autorité de certification du capteur).

Figure 23: Activer la relocalisation de l'agent



Étape 5 Cliquez sur **Enable Agent Rehoming** ((activer la relocalisation de l'agent).

La configuration est enregistrée. Le bouton Rehome (Relocalisation) s'affiche en haut à droite.

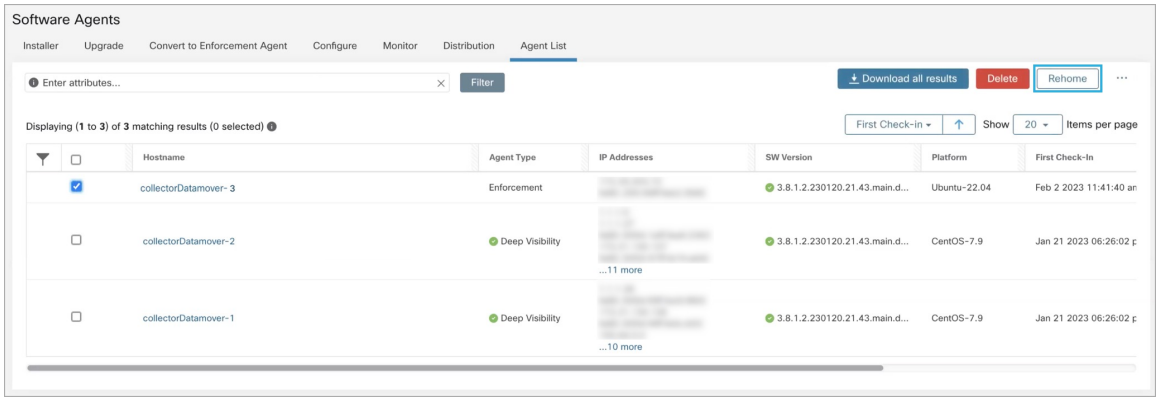
Sélectionner les agents à relocaliser

Procedure

Étape 1 Sélectionnez un agent.

Étape 2 Cliquez sur **Rehome** (Relocaliser).

Figure 24: Sélectionner les agents à relocaliser



Étape 3 Cliquez sur **Yes** (Oui) pour confirmer.

Désactiver la relocalisation

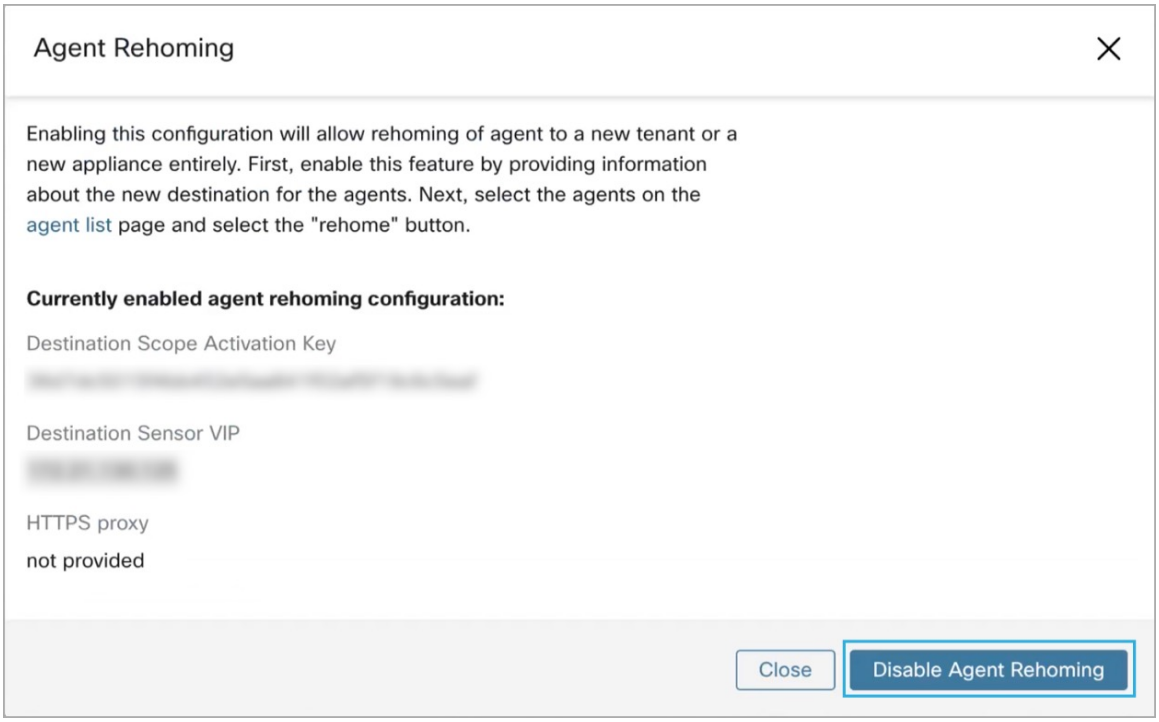
Note Si plusieurs utilisateurs se déplacent vers un un logiciel-service SaaS ou à partir de celui-ci, l'administrateur du site doit déplacer chaque détenteur ou appareil séparément. Pour ce faire, désactivez la relocalisation pour effacer les paramètres, puis activez la relocalisation pour le nouvel utilisateur.

Procedure

Étape 1 Cliquez sur l'icône de menu et sélectionnez **Rehome Agents** (Relocaliser les agents).

Étape 2 Dans la fenêtre **Agent Rehoming** (Relocalisation de l'agent), cliquez sur **Disable Agent Rehoming** (Désactiver la relocalisation de l'agent).

Figure 25: Désactiver la relocalisation de l'agent



Générer un jeton d'agent

Dans le profil de configuration de l'agent, vous pouvez activer la protection de service pour empêcher la désinstallation, la désactivation et l'arrêt des services d'agent Windows. Pour apporter des modifications aux agents, vous pouvez désactiver cette protection dans le profil de configuration de l'agent. Toutefois, si vous ne parvenez pas à désactiver la protection en raison de problèmes de connectivité, vous pouvez générer un jeton d'agent pour désactiver la protection de service sur les charges de travail. Le jeton est valide pendant 15 minutes.

Rôles pris en charge pour générer et récupérer des jetons d'agent :

- **Administrateurs de site** : pour les grappes ou les détenteurs.
- **Service à la clientèle** : pour les détenteurs.
- **Programme d'installation de l'agent** : pour les jetons propres à l'agent.

Note Vous pouvez générer des jetons d'agent basés sur le temps uniquement pour les agents logiciels basés sur le système d'exploitation Windows.

Pour générer et télécharger des jetons d'agent, procédez comme suit :

Procedure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)** > **Agent List (Liste des agents)**.

Selon vos besoins, vous pouvez choisir l'un des types de jetons d'agent : grappe, détenteur ou propre à l'agent. Pour le jeton propre à l'agent, passez à l'étape 5.

Étape 2 Cliquez sur l'icône de menu et sélectionnez **Agent Token** (Jeton propre à l'agent).

Note L'option de **jeton propre à l'agent** est uniquement visible pour les administrateurs de site ou les rôles d'utilisateur du service d'assistance à la clientèle.

Étape 3 Sélectionnez un type de jeton

- Token For Cluster (jeton pour la grappe) : Cette option est visible uniquement par les administrateurs de site et le jeton est applicable à tous les agents.
- Token For Tenant (Jeton pour le détenteur) : applicable pour les agents d'un détenteur sélectionné.

Étape 4 Pour télécharger la clé de jeton, cliquez sur **Télécharger le jeton**.

Étape 5 Pour afficher et télécharger les détails de la clé de jeton d'un agent spécifique :

a) Allez à l'onglet **Agent List** (Liste des agents) et cliquez sur l'agent requis. Sous **Agent Details (Détails de l'agent)** > **Agent Token(Jeton de l'agent)** , vous pouvez afficher la clé du jeton et les détails d'expiration du jeton.

b) Pour télécharger le jeton propre à l'agent, cliquez sur **Télécharger le jeton**.

What to do next

Après avoir téléchargé le fichier de jeton de l'agent, exécutez la commande suivante sur l'agent pour désactiver la protection de service : `"C:\Program Files\Cisco Tetration\TetSen.exe" -unprotect <token>`, où `token` est le jeton de l'agent téléchargé.

Une fois la protection du service désactivée à l'aide d'un jeton, elle peut être réactivée automatiquement lorsque le service redémarre et se connecte à la grappe Cisco Secure Workload.

Changement de l'adresse IP de l'hôte lorsque la mise en application est activée

La modification de l'adresse IP sur les hôtes lorsque l'application est activée peut avoir un impact si l'adresse IP de l'hôte est visible dans les règles de pare-feu de l'hôte et que le paramètre Règle collectrice est défini sur Refuser. Dans ce scénario, il est recommandé de suivre les étapes suivantes pour modifier l'adresse IP de l'hôte :

Procedure

Étape 1 Dans l'interface utilisateur Cisco Secure Workload, créez un nouveau profil de configuration d'agent avec la mise en application désactivée.

Étape 2 Créez un intent avec la liste des hôtes qui ont besoin d'un changement d'adresse IP avec leur ancienne et leur nouvelle adresse IP.

Étape 3 Appliquez le nouveau profil de configuration d'agent à l'intent et enregistrez l'intent.

Étape 4 La mise en application doit être désactivée pour ces hôtes sélectionnés.

Étape 5 Modifiez l'adresse IP de ces hôtes.

Étape 6 Sur l'interface utilisateur Cisco Secure Workload, mettez à jour les filtres de la portée avec la nouvelle adresse IP de ces hôtes.

Étape 7 Vérifiez le changement d'adresse IP sous l'onglet Interfaces de la page de profil de charge de travail de l'agent. Dans l'onglet « Policies » (politiques), assurez-vous que les politiques sont générées avec la nouvelle adresse IP.

Étape 8 Supprimez l'intent ou le profil créé ci-dessus.

Étape 9 Si la mise en application était désactivée dans le profil de configuration de l'agent d'origine pour la portée, activez-la.

Mise à niveau des agents logiciels

Mettre à niveau les agents à partir de l'interface utilisateur

Les agents peuvent être mis à niveau à l'aide du flux de travaux d'intent de configuration d'agent, comme décrit ici - Configuration de l'agent logiciel. Lors de la configuration d'un profil de configuration d'agent, il existe une option **Auto Upgrade** (mise à niveau automatique) qui peut être activée ou désactivée. Si l'option est activée, les agents correspondant aux critères du filtre d'inventaire sont automatiquement mis à niveau vers la dernière version disponible.

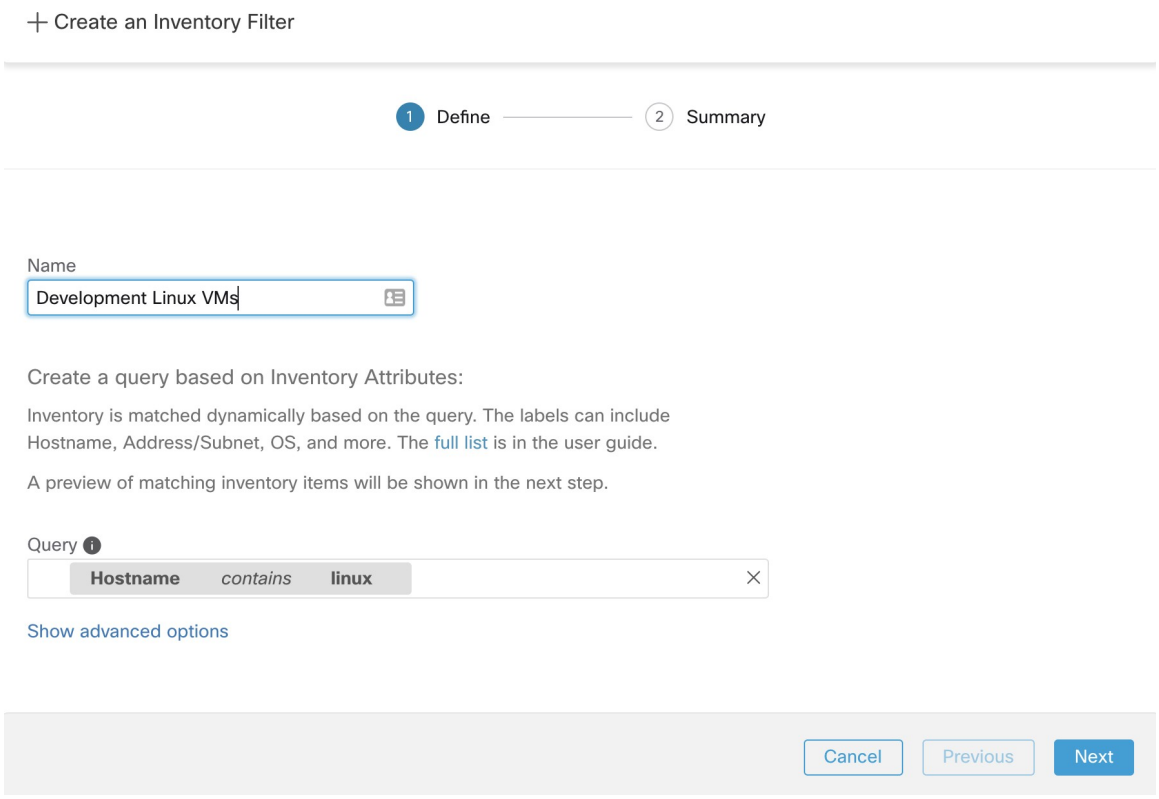
Sur la page **Software Agents (Agents logiciels)** > **Agent List (Liste d'agents)**, les agents logiciels dont les versions sont obsolètes sont mis en évidence par un panneau d'avertissement sous la colonne **SW Version** (version logicielle). Il est important de mettre à niveau ces agents à la dernière version disponible sur la grappe.

Pour utiliser le flux de travaux d'intent de configuration d'agent logiciel afin de configurer la mise à niveau de l'agent logiciel :

Procedure

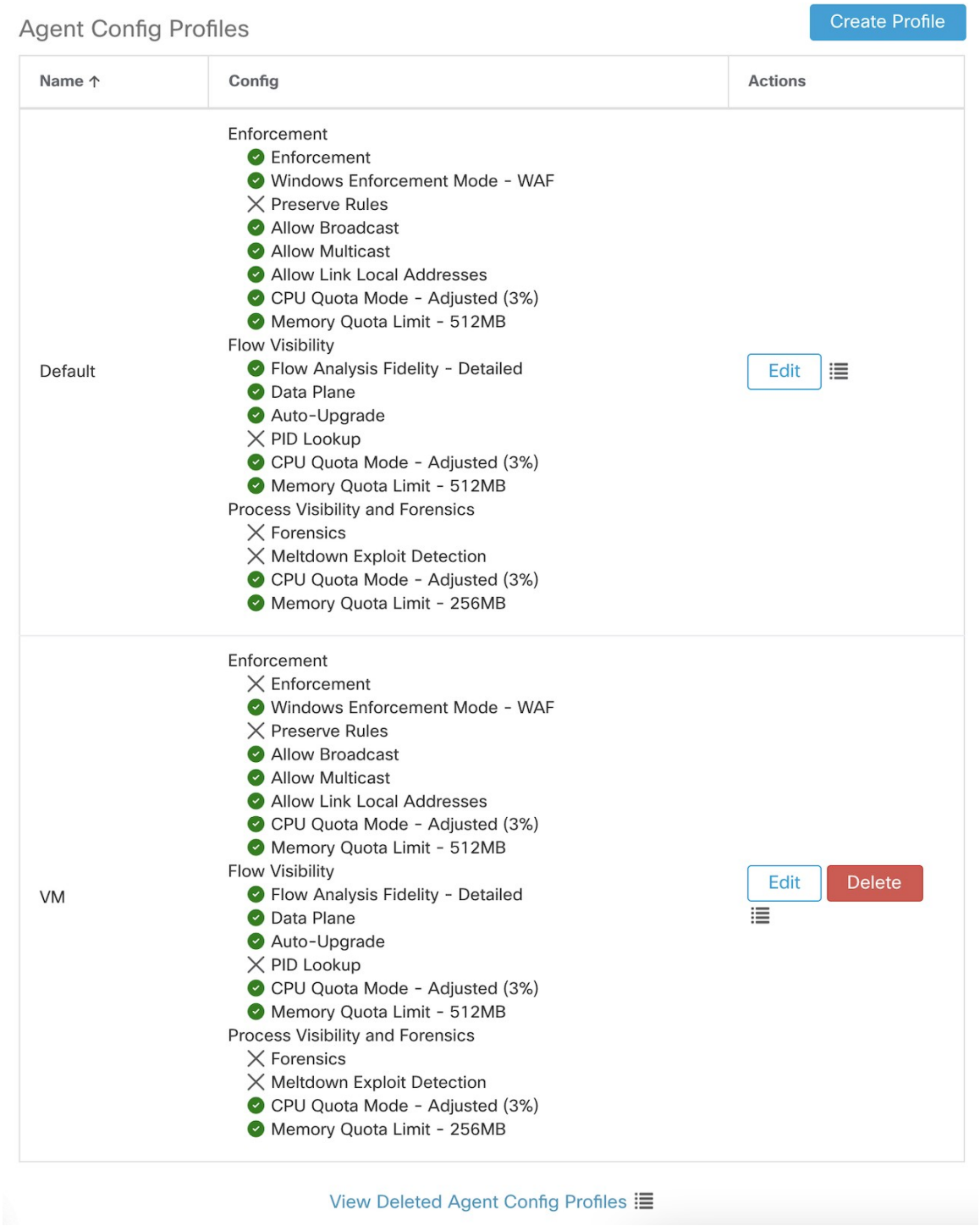
Étape 1 Créez un filtre d'inventaire sur la page **Inventory Filters** (Filtres d'inventaire). Pour en savoir plus, consultez Filtres.

Figure 26: Filtre d'inventaire



Étape 2 Créez un profil de configuration d'agent pour les agents sélectionnés par le filtre d'inventaire. Vous pouvez également activer l'option **Auto Upgrade** (mise à niveau automatique) pour mettre automatiquement à niveau les agents sélectionnés.

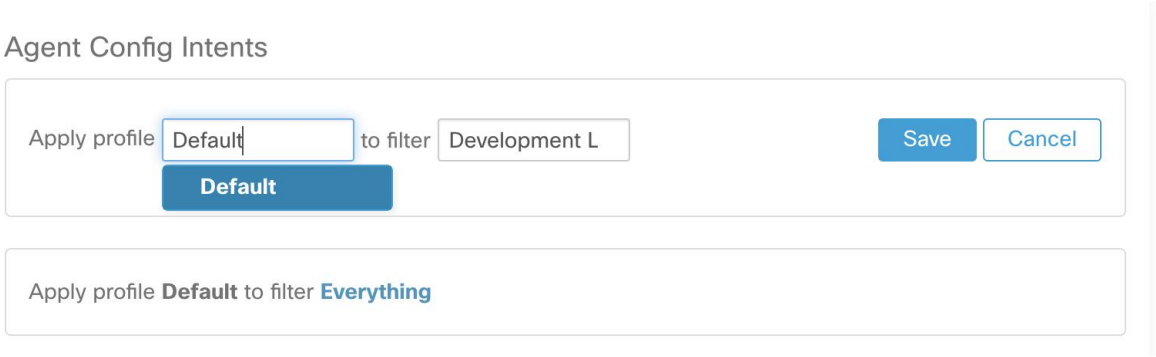
Figure 27: Configuration de l'agent



Étape 3 Créez un intent de configuration d'agent pour appliquer le profil de configuration aux agents sélectionnés à l'aide du filtre d'inventaire. Si l'option de mise à niveau automatique est activée, les agents sélectionnés sont automatiquement mis à niveau.

La mise à niveau d'un agent après l'application d'un profil d'agent prend normalement jusqu'à 30 minutes.

Figure 28: Intent de configuration de l'agent



Note Le paramètre de mise à niveau automatique du profil d'agent par défaut s'applique à ERSPAN.

Mise à niveau manuelle de l'agent

La section suivante explique comment mettre à niveau manuellement les agents sans utiliser le flux de travail d'intent de configuration de capteur.

Procedure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)**.

Étape 2 Cliquez sur l'onglet **Upgrade** (Mise à niveau).
Les agents de visibilité approfondie et d'application sont affichés, et pour chaque agent, seules les versions les plus récentes vers lesquelles l'agent peut être mis à niveau sont répertoriées. Par défaut, la dernière version est sélectionnée.

Étape 3 Pour filtrer des agents spécifiques, saisissez votre requête de recherche dans la zone de filtre. Par exemple, saisissez Platform = CentOS-7.6.

Étape 4 Sélectionnez les agents à mettre à niveau à la version sélectionnée et cliquez sur **Upgrade** (Mettre à niveau).

Note Dans des circonstances normales, il est fortement recommandé d'autoriser l'agent à effectuer automatiquement la mise à niveau et il s'agit de la seule méthode de mise à niveau prise en charge. Si vous souhaitez contrôler la mise à niveau en téléchargeant manuellement la dernière version et en la déployant directement sur les agents qui s'exécutent sur les charges de travail, assurez-vous de suivre les mesures de sécurité.

Mettre à niveau le comportement de l'agent Kubernetes/Openshift

Les agents installés sur des nœuds Kubernetes ou OpenShift à l'aide du script d'installation du daemonset peuvent se mettre à niveau eux-mêmes. Le processus de mise à niveau est contrôlé soit par l'option de mise à niveau automatique, soit par le déclenchement manuel d'une mise à niveau pour n'importe quel nœud de la

grappe Kubernetes/Openshift Le mécanisme de mise à niveau dans cet environnement est de mettre à niveau l'image Docker dans les spécifications du daemonset ce qui signifie qu'une mise à niveau d'un agent affecte tous les agents couverts par le daemonset, comme l'explique le paragraphe suivant.

Lorsqu'un ensemble de spécifications de Pods change, Kubernetes/OpenShift déclenche un arrêt progressif, récupère la ou les nouvelles images Docker et démarre les pods d'agents Cisco Secure Workload sur TOUS les nœuds de la grappe Kubernetes/Openshift. Ainsi, les agents seront mis à niveau sur d'autres nœuds, même si la politique autorisant les mises à niveau ne s'applique qu'à un sous-ensemble des nœuds de la grappe.

Si la mise à niveau automatique est désactivée pour tous les nœuds, la mise à niveau manuelle est possible en téléchargeant un nouveau script d'installation et en réexécutant l'installation. Le script d'installation détecte automatiquement le cas d'une nouvelle installation par rapport à la mise à niveau d'une installation existante et travaillera pour mettre à niveau manuellement les pods du daemonset lorsqu'il détecte qu'une installation est déjà en place.

Suppression des agents logiciels

Supprimer un agent Linux de visibilité approfondie ou d'application

Installation basée sur le RPM :

1. Exécutez la commande : **rpm -e tet-sensor**

L'événement de désinstallation de l'agent est communiqué à la grappe et l'agent est marqué comme désinstallé sur la page **Software Agent** (agents logiciels).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (agent logiciel). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

Note Par défaut, la **période de nettoyage** est désactivée.

Installation basée sur Ubuntu .deb :

La nouvelle installation des agents Ubuntu utilise désormais le format natif .deb.

1. Exécutez la commande : **dpkg –purge tet-sensor**

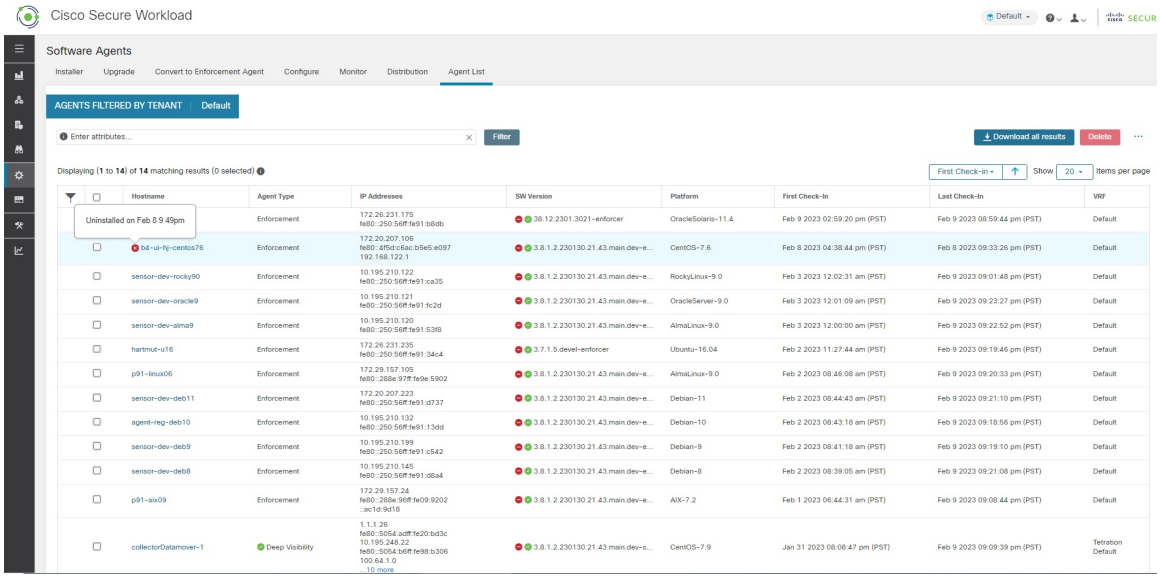
L'événement de désinstallation de l'agent est communiqué à la grappe et l'agent est marqué comme désinstallé sur la page **Software Agent** (agents logiciels).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (agents logiciels). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

Note

- Par défaut, la **période de nettoyage** est désactivée.
- Pendant les opérations de l'agent, il est possible que certains modules du noyau soient chargés automatiquement par ce dernier. Par exemple, si l'application est activée sous Linux, les modules Netfilter peuvent être chargés. Les agents n'ont pas de liste des modules chargés par le noyau. Par conséquent, pendant la désinstallation de l'agent, il est impossible de décharger les modules du noyau.
- Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

Figure 29: Alerte de désinstallation de l'agent



Suppression d'un agent Windows de visibilité approfondie/de mise en application

Il existe deux options pour désinstaller les agents Cisco Secure Workload :

Procedure

Étape 1 Accédez à Panneau de configuration/Programmes/Programmes et fonctionnalités, puis désinstallez **Cisco Secure Workload Agent** (Agent Cisco Tetration).

Étape 2 Vous pouvez également exécuter le raccourci **Uninstall.lnk** dans **« C:\Program Files\Cisco Tetration »**

Étape 3 Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

L'événement de désinstallation de l'agent sera communiqué à la grappe et l'agent sera marqué comme désinstallé sur la page **Software Agent** (Agent logiciel).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (Agent logiciel). Sinon , l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

Note Par défaut, la **période de nettoyage** est désactivée.

Note
- Si Npcap a été installé lors de l'installation de l'agent, il sera également désinstallé.
- Par défaut, les fichiers journaux, les fichiers de configuration et les certificats ne seront pas supprimés lors de la désinstallation. Si vous souhaitez les supprimer, exécutez le raccourci **UninstallAll.lnk** dans le même dossier.

Supprimer un agent AIX de visibilité approfondie ou d'application

Procedure

Exécutez la commande : **« installp -u tet-sensor »**.

L'événement de désinstallation de l'agent sera communiqué à la grappe et l'agent sera marqué comme désinstallé sur la page **Software Agent** (Agent logiciel).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (Agent logiciel). Sinon , l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

Note
- Par défaut, la **période de nettoyage** est désactivée.
- L'agent de visibilité approfondie est contrôlé par le contrôleur de ressources système en tant que tet-sensor. Il est possible de le démarrer, l'arrêter, le redémarrer et le supprimer. Le service est rendu persistant avec inittab en tant que tet-sen-engine.
- L'agent d'application est contrôlé par le contrôleur de ressources système en tant que tet-enforcer. Il est possible de le démarrer, l'arrêter, le redémarrer et le supprimer. Le service est rendu persistant avec inittab en tant que tet-enf-engine.
- Pendant les opérations de l'agent, il est possible que certains modules du noyau soient chargés automatiquement par ce dernier. Par exemple, si l'application est activée dans AIX, les modules ipfilter sont chargés. Les agents n'ont pas de liste des modules chargés par le noyau. Par conséquent, pendant la désinstallation de l'agent, il est impossible de décharger les modules du noyau.
- Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

Supprimer l'agent Universal Linux

Procedure

Étape 1 Exécutez le script de désinstallation : **« /usr/local/tet-light/uninstall.sh »**

Étape 2 Supprimez l'agent de l'interface utilisateur dans la page **Software Agent (agent logiciel).**

Supprimer l'agent Windows universel

Procedure

Étape 1 Exécutez le script de désinstallation : **« C:\Program Files\Cisco Tetration\Lightweight Sensor\uninstall.cmd »**

Étape 2 Supprimez l'agent de l'interface utilisateur dans la page **Software Agent (agent logiciel).**

Supprimer un agent d'application Kubernetes ou OpenShift

Procedure

Étape 1 Localisez le script du programme d'installation d'origine ou téléchargez un nouveau script à partir de l'interface utilisateur Cisco Secure Workload.

Étape 2 Exécutez l'option de désinstallation : **install.sh –uninstall**. Les mêmes considérations s'appliquent que lors de l'installation.

- Pris en charge uniquement sur les architectures Linux x86_64.
- ~/.kube/config contient un utilisateur d'informations d'authentification d'administrateur ou utilisez l'option –kubeconfig pour pointer vers le fichier d'informations d'authentification de l'administrateur kubectl.

Étape 3 Supprimez les agents pour tous les nœuds Kubernetes de l'interface utilisateur sur la page **Software Agent** (Agents logiciels)

Supprimer un agent de visibilité approfondie Solaris

Procedure

Étape 1 Exécutez la commande : `pkg uninstall tet-sensor`

Étape 2 Supprimez l'agent dans la page **Software Agent** (Agent logiciel).

Données collectées et exportées par les agents de charge de travail

Cette section décrit les principaux composants d'un agent logiciel, la façon dont il est enregistré auprès des services dorsaux (backend) et les données qui sont collectées et exportées vers la grappe à des fins d'analyse.

Inscription

Une fois que l'agent a été installé avec succès sur le système, il doit s'inscrire auprès des services dorsaux pour obtenir un identifiant unique valide. Les renseignements suivants sont envoyés avec la demande d'enregistrement :

- Nom d'hôte
- BIOS-UUID
- Informations sur la plateforme (telle que CentOS-6.5)
- Certificat client généré automatiquement (généré avec la commande openssl)
- Type d'agent (visibilité ou application)

Si l'agent ne parvient pas à obtenir un ID valide du serveur, il réessaiera jusqu'à ce qu'il en obvienne. Il est très important que l'agent soit enregistré, sinon toutes les communications ultérieures avec d'autres services (comme les collecteurs) seront rejetées.

Mise à niveau de l'agent

Périodiquement (environ toutes les 30 minutes), l'agent envoie un message au service de serveur principal (backend) pour signaler sa version actuelle. Le service de serveur principal utilise l'ID de l'agent et sa version actuelle pour décider si un nouveau paquet est disponible pour l'agent. Les renseignements suivants sont envoyés :

- ID de l'agent (obtenu après un enregistrement réussi)
- Version actuelle de l'agent

Serveur de configuration

Les agents exportent les informations suivantes vers le serveur de configuration configuré :

- Nom d'hôte
- ID de l'agent (obtenu après un enregistrement réussi)
- Liste des interfaces, chacune d'entre elles comprend
  1. Nom de l'interface

2. Famille IP (IPv4 ou IPv6)
3. Adresses IP
4. Masque réseau
5. Adresses MAC
6. Indice d'interface

Dès que une propriété d'interface change (comme l'adresse IP d'une interface existante change, ou une nouvelle interface apparaît), cette liste est actualisée et signalée au serveur de configuration.

Network flow

Network Flow information is the summarization of all packets flowing through the system. There are two modes of capturing flow information: Detailed and Conversation. By default the Detailed mode of capture is used. The captured flows are exported to collector, the exported information includes:

- Flow identifier: uniquely identify the network flow. It includes the general information such as: IP protocol, source and destination IP, and layer 4 ports
- IP Information: contains information seen in IP header, such as: TTL, IP flags, Packet ID, IP options and Fragmentation flags
- TCP Information: contains information seen in TCP header, such as: sequence number, Ack number, TCP options, Rcvd windows size
- Flow Information: flow's statistics (such as: total packets, total bytes, TCP flags statistics, packet length statistics and socket statistics), interface index from which flow was observed, flow's start time and end time

In Conversation mode, agents will only export TCP flows that are bi-directional in nature along with other connectionless flows. Conversation mode is supported for Windows, AIX and Linux platforms. For more information on Conversation mode, see Conversation Mode.

Note In K8s environment, correlation of Pod/Host flows will not be done in Conversation mode.

Note that in either mode agent will not export the following flows:

- ARP/RARP conversations
- Agent's flows to collectors

Renseignements sur la machine

Les renseignements sur la machine décrivent tous les processus en cours d'exécution sur l'hôte. En outre, ils contiennent des informations sur le réseau associées aux processus et sur la commande utilisée pour lancer les processus. Les renseignements sur la machine sont exportés toutes les minutes et comprennent les éléments suivants :

- Identifiant de processus
- Identifiant de l'utilisateur : propriétaire du processus

- ID du processus parent
- Chaîne de commande utilisée pour lancer le processus
- Renseignements sur le socket : protocole (comme UDP ou TCP), type d'adresse : IPv4 ou IPv6, adresse IP source et de destination, ports source et de destination, état TCP, heures de début et de fin du processus, chemin d'accès au fichier binaire
- Renseignements criminalistiques : pour en savoir plus, consultez la section Compatibilité, on page 598.

Statistiques des agents

L'agent effectue le suivi de diverses statistiques, y compris les statistiques du système et les siennes, notamment :

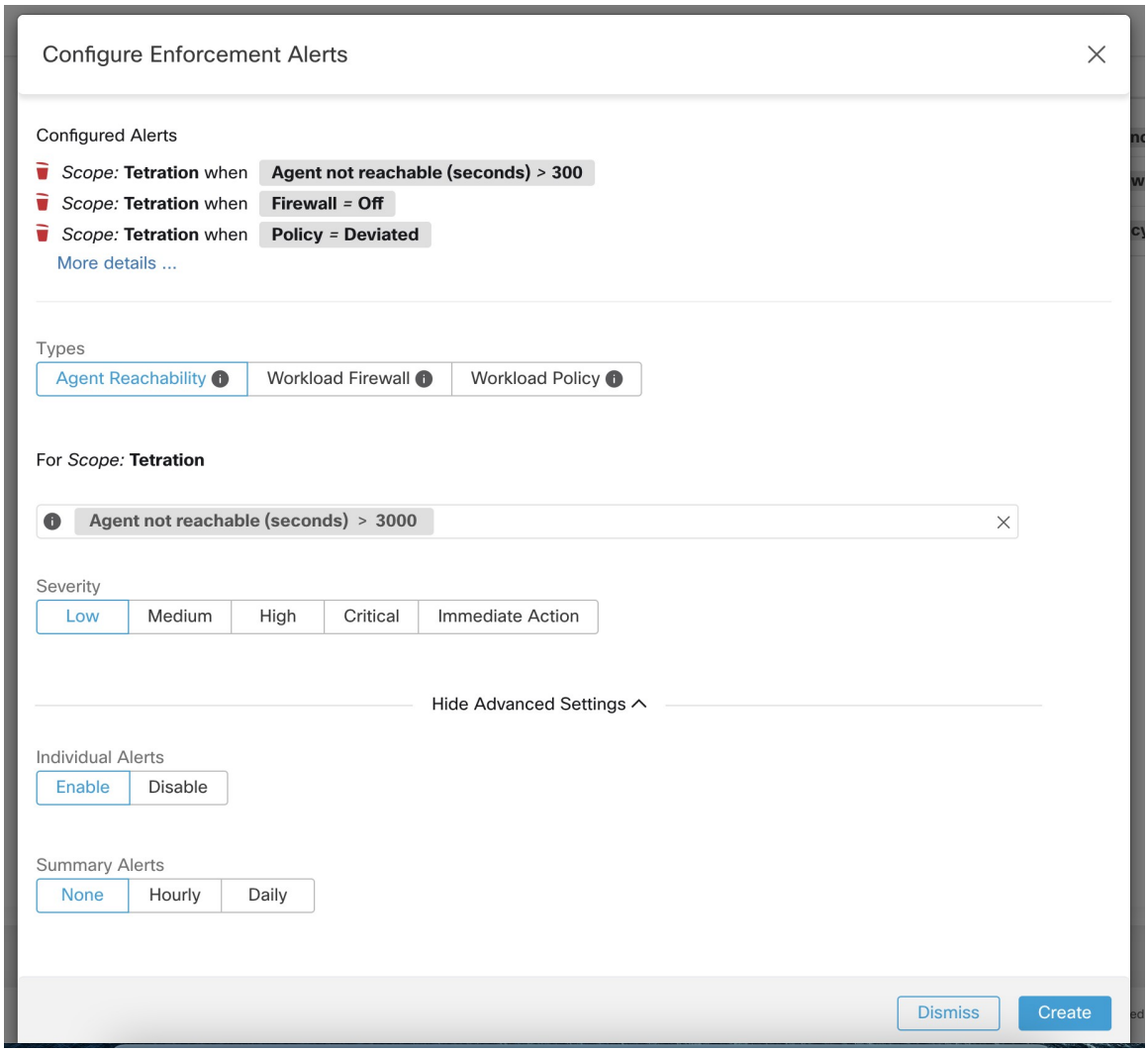
- Heure de début et durée de disponibilité de l'agent
- Durée d'exécution de l'agent en mode utilisateur et en mode noyau
- Le nombre de paquets reçus et abandonnés
- Nombre de connexions SSL réussies et échouées
- Flux total de paquets et d'octets
- Total des flux et paquets exportés vers les collecteurs
- Utilisation de la mémoire et de la CPU de l'agent

Alertes de mise en application

Il existe trois types d'alertes de mise en application :

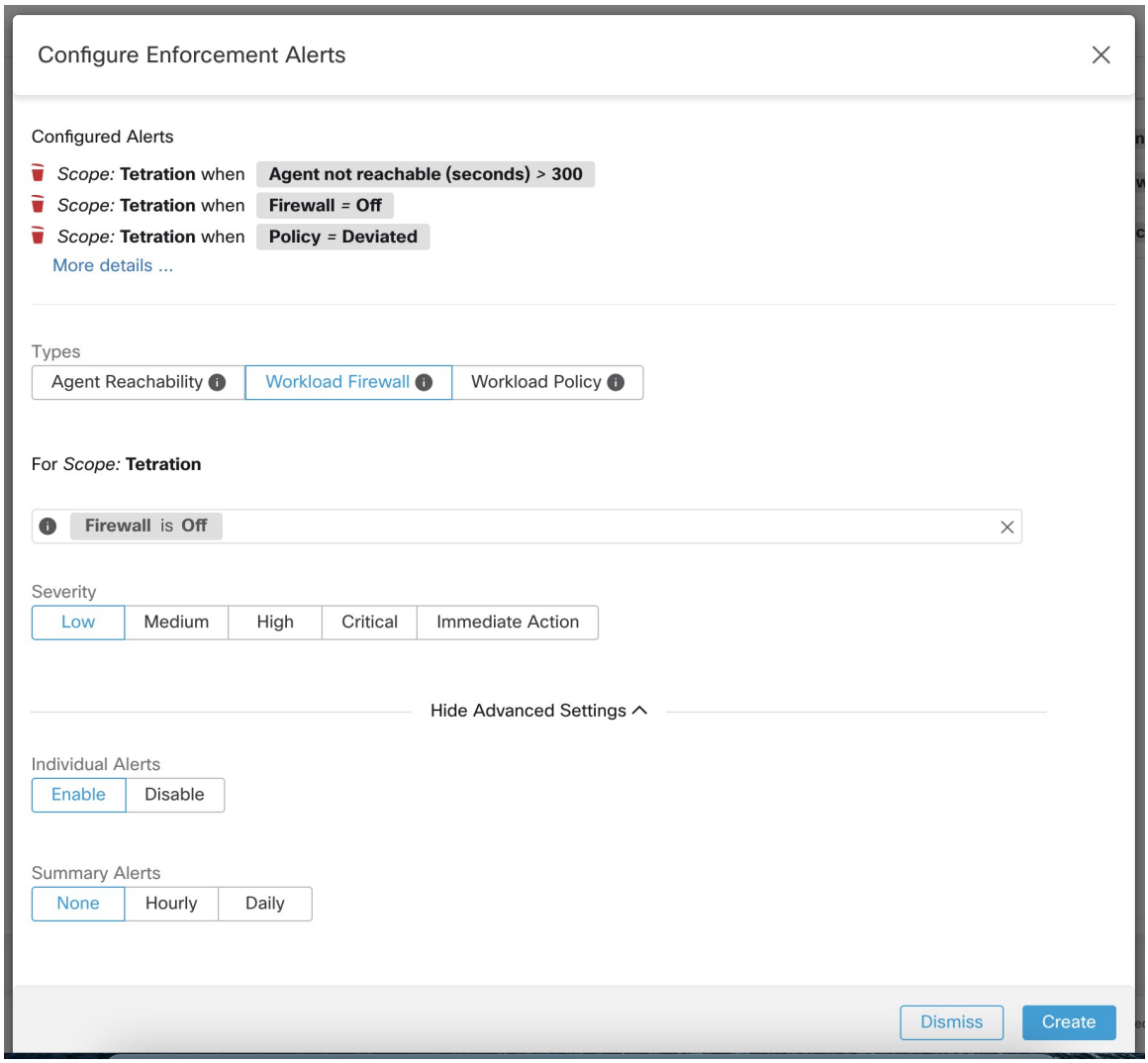
- Accessibilité de l'agent

  Cette alerte détecte lorsque l'agent n'est pas accessible. Cette alerte se déclenche si l'agent n'a pas communiqué avec la grappe Cisco Secure Workload pendant une durée supérieure au nombre de secondes configuré.



- Pare-feu de charge de travail

  Cette alerte se déclenche si l'application est configurée sur un charge de travail mais que le pare-feu est détecté comme désactivé, car cette condition empêchera l'agent Cisco Secure Workload d'appliquer les politiques de trafic.



- Politique de charge de travail

  Cette alerte se déclenche si les règles du pare-feu de charge de travail sont différentes des politiques Cisco Secure Workload applicables à cette charge de travail (les « politiques concrètes » de la charge de travail)

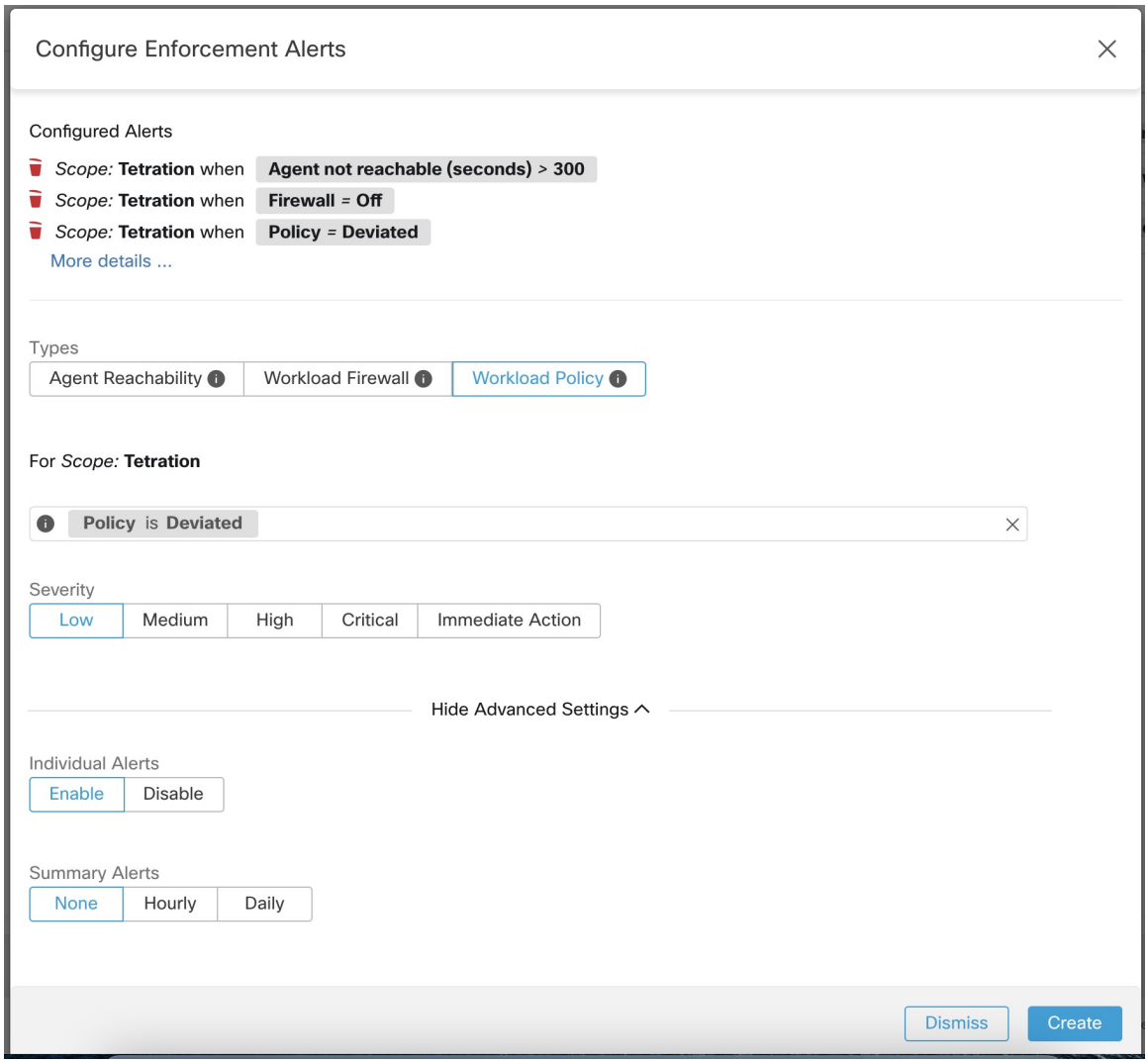
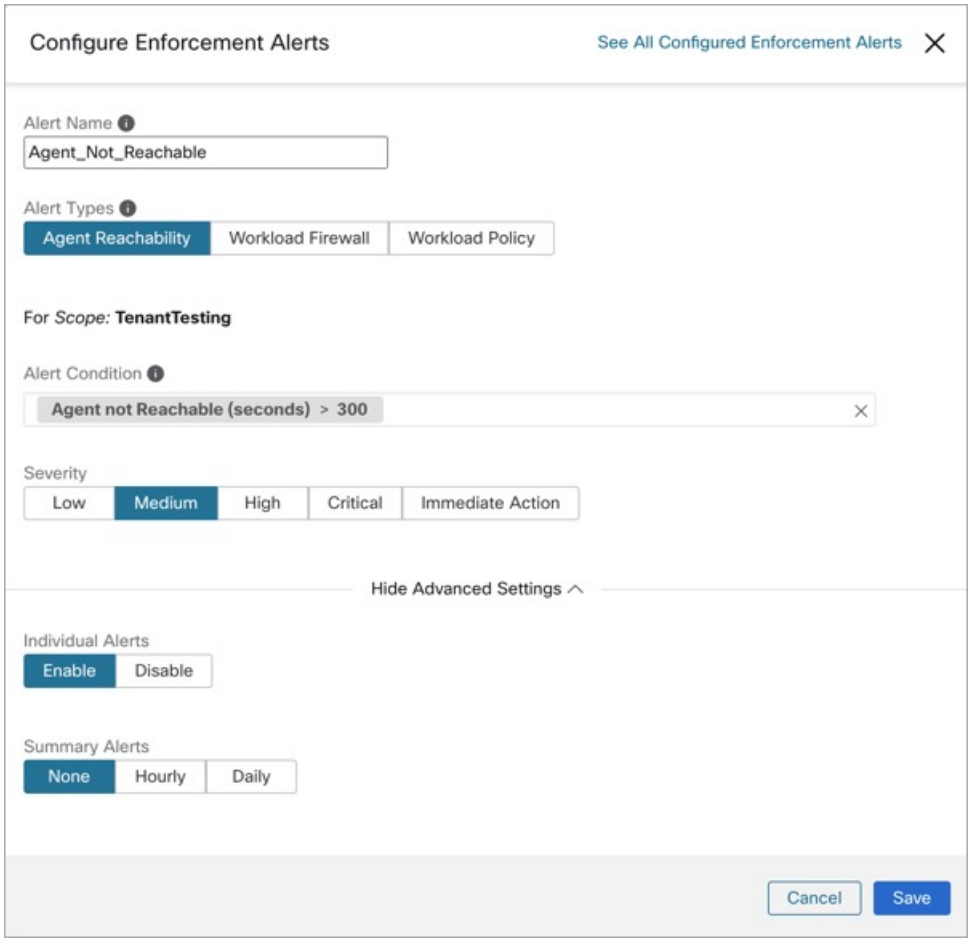

Configure Enforcement Alerts
Configured Alerts
Scope: Tetration when Agent not reachable (seconds) > 300
Scope: Tetration when Firewall = Off
Scope: Tetration when Policy = Deviated
More details ...
Types
Agent Reachability
Workload Firewall
Workload Policy
For Scope: Tetration
Policy is Deviated
Severity
Low
Medium
High
Critical
Immediate Action
Hide Advanced Settings
Individual Alerts
Enable
Disable
Summary Alerts
None
Hourly
Daily
Dismiss
Create

Figure 30: Types d'alertes de mise en application



Vous pouvez définir la gravité de l'alerte ainsi que d'autres paramètres de configuration par type.

Pour configurer les alertes de mise application, consultez Configurer les alertes, on page 673.

Figure 31: Configuration des alertes de mise en application

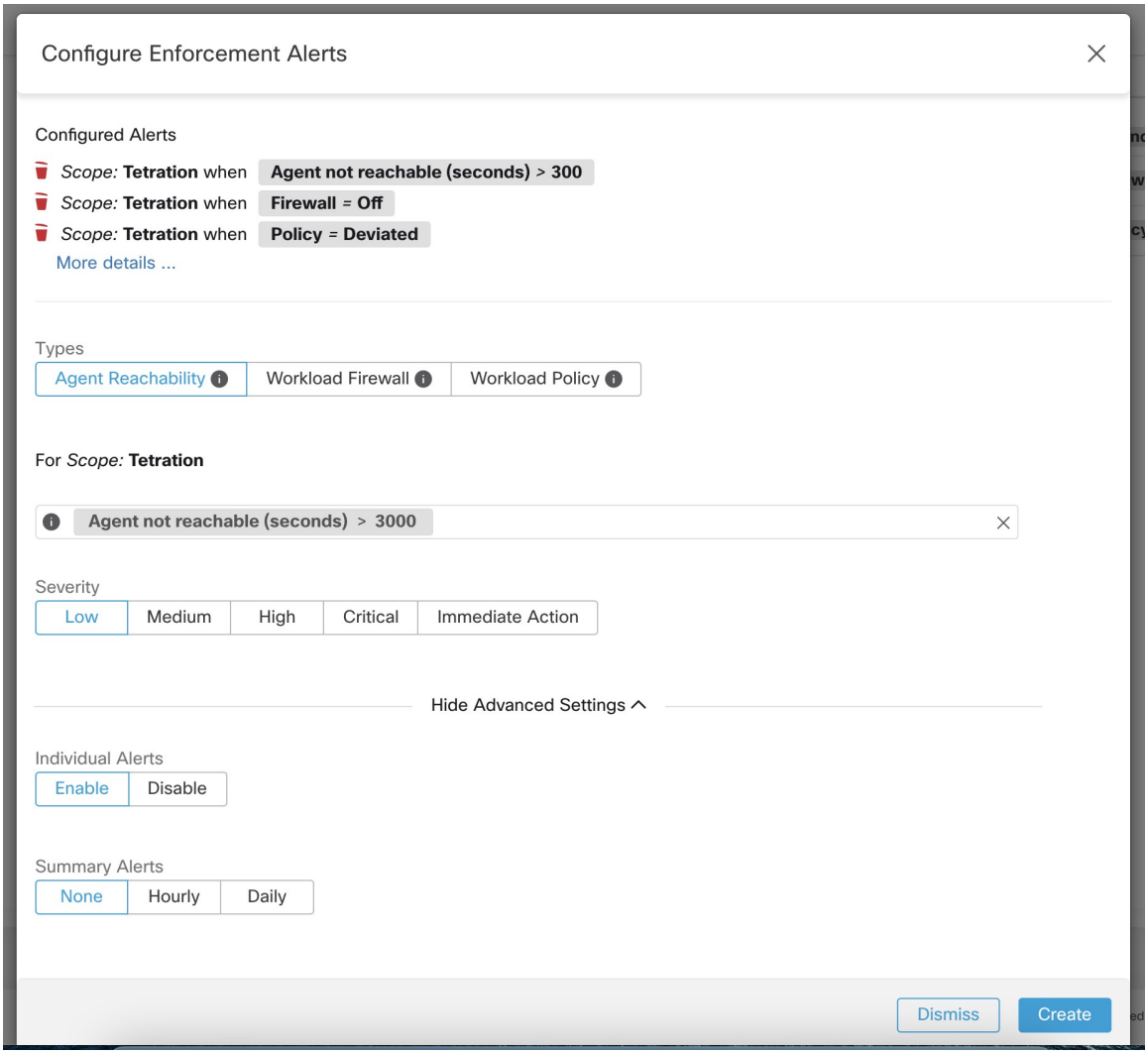


Figure 32: Affichage des alertes de mise en application configurées sur la page de configuration des alertes

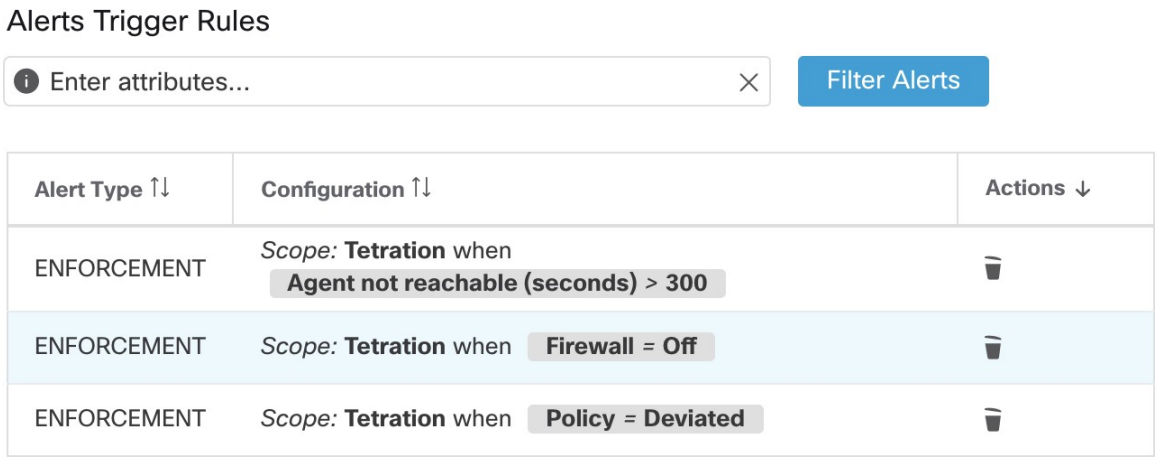


Figure 33: Afficher les alertes de mise en application configurées

Détails des alertes de l'interface utilisateur d'application

Figure 34: Détails de l'alerte d'application

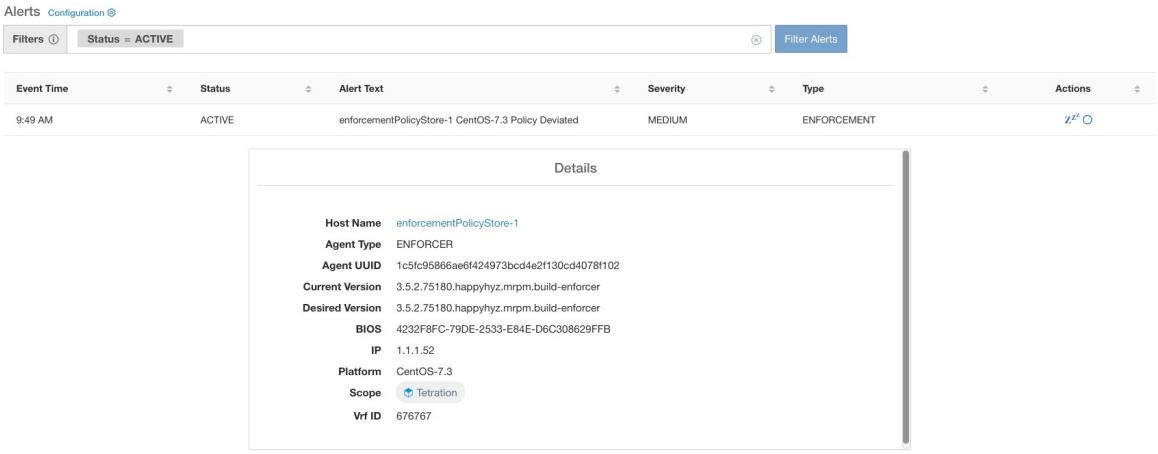
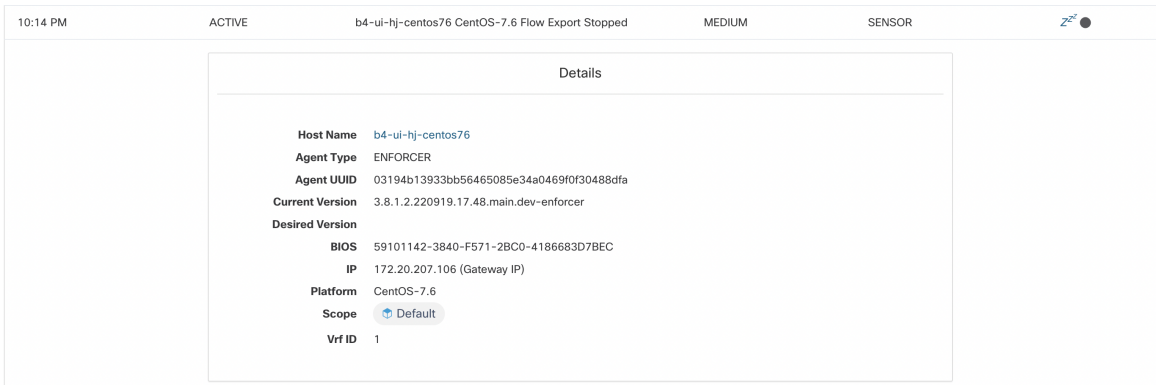


Figure 35: Détails d'alertes d'application lorsque le serveur mandataire est activé sur l'hôte



Détails de l'alerte d'application

Consultez Structure commune des alertes pour obtenir la structure générale des alertes et des informations sur les champs. Le champ *alert_détails* est structuré et contient les sous-champs suivants pour les alertes de mise en application

Champ	Type d'alerte	Format	Explication
Type d'agent	*tous*	chaîne	« ENFORCER » (APPLICATEUR) ou « SENSOR » (CAPTEUR) selon le type d'installation
Nom de l'hôte :	*tous*	chaîne	Nom de l'hôte sur lequel l'agent est déployé
IP	*tous*	chaîne	Adresse IP du nœud ou de la passerelle
Biographies	*tous*	chaîne	UUID BIOS du nœud
Observations	*tous*	chaîne	Renseignements sur la plateforme ou le système d'exploitation du nœud
Version actuelle	*tous*	chaîne	Version du logiciel de l'agent sur le nœud
Version souhaitée	*tous*	chaîne	Version du logiciel souhaitée pour l'agent
LastConfigFetchAt	*tous*	nombre entier	Horodatage Unix de la dernière fois que l'agent a envoyé une requête https

Exemple de détails_alertes pour une alerte de mise en application

```
{
  "AgentType":"ENFORCER",
  "Bios":"72EF1142-03A2-03BC-C2F8-F600567BA320",
  "CurrentVersion":"3.5.1.1.mrpm.build.win64-enforcer",
  "DesiredVersion":"",
  "HostName":"win2k12-production-db",
  "IP":"172.26.231.193",
  "Platform":"MSServer2012R2Standard"
}
```

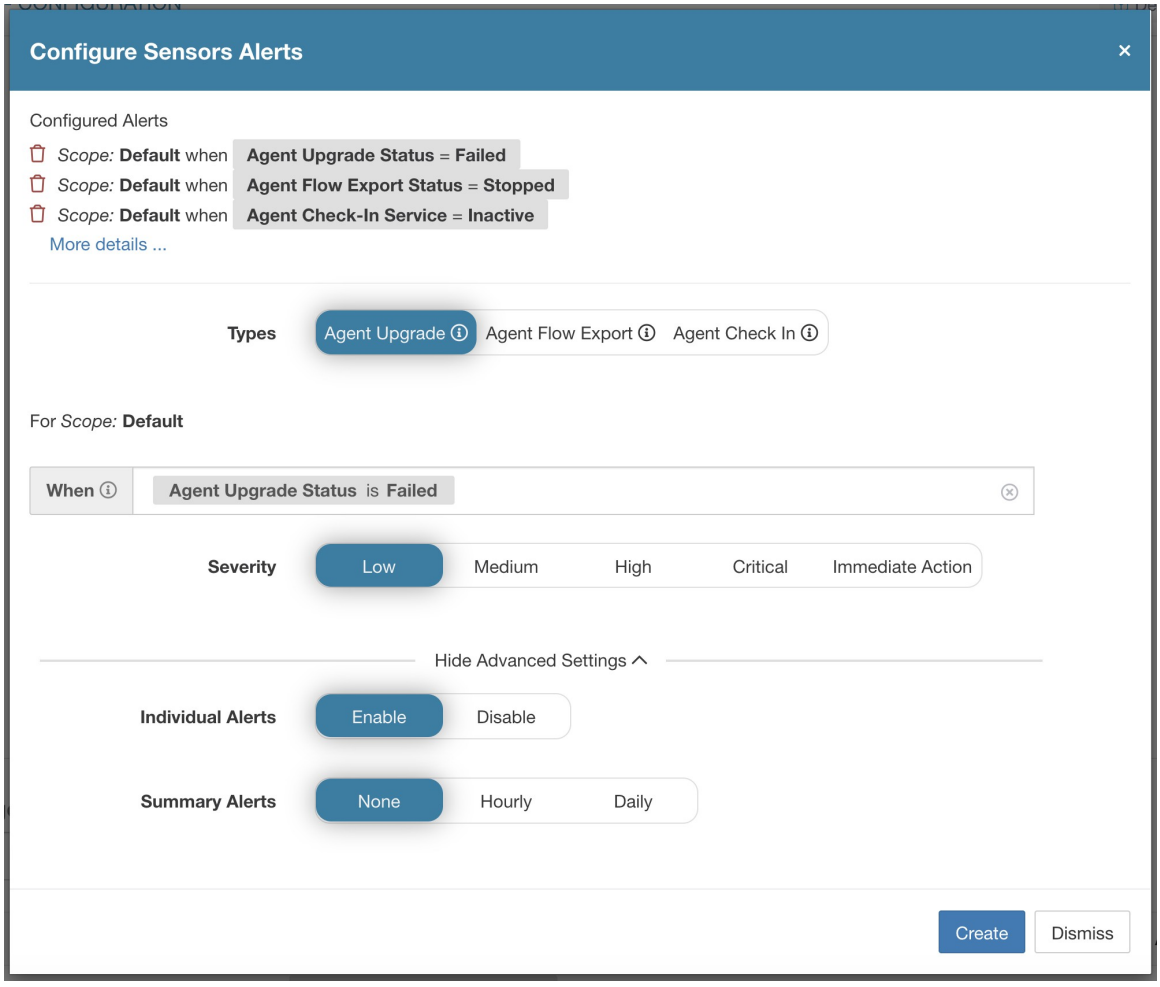
Alertes de capteurs

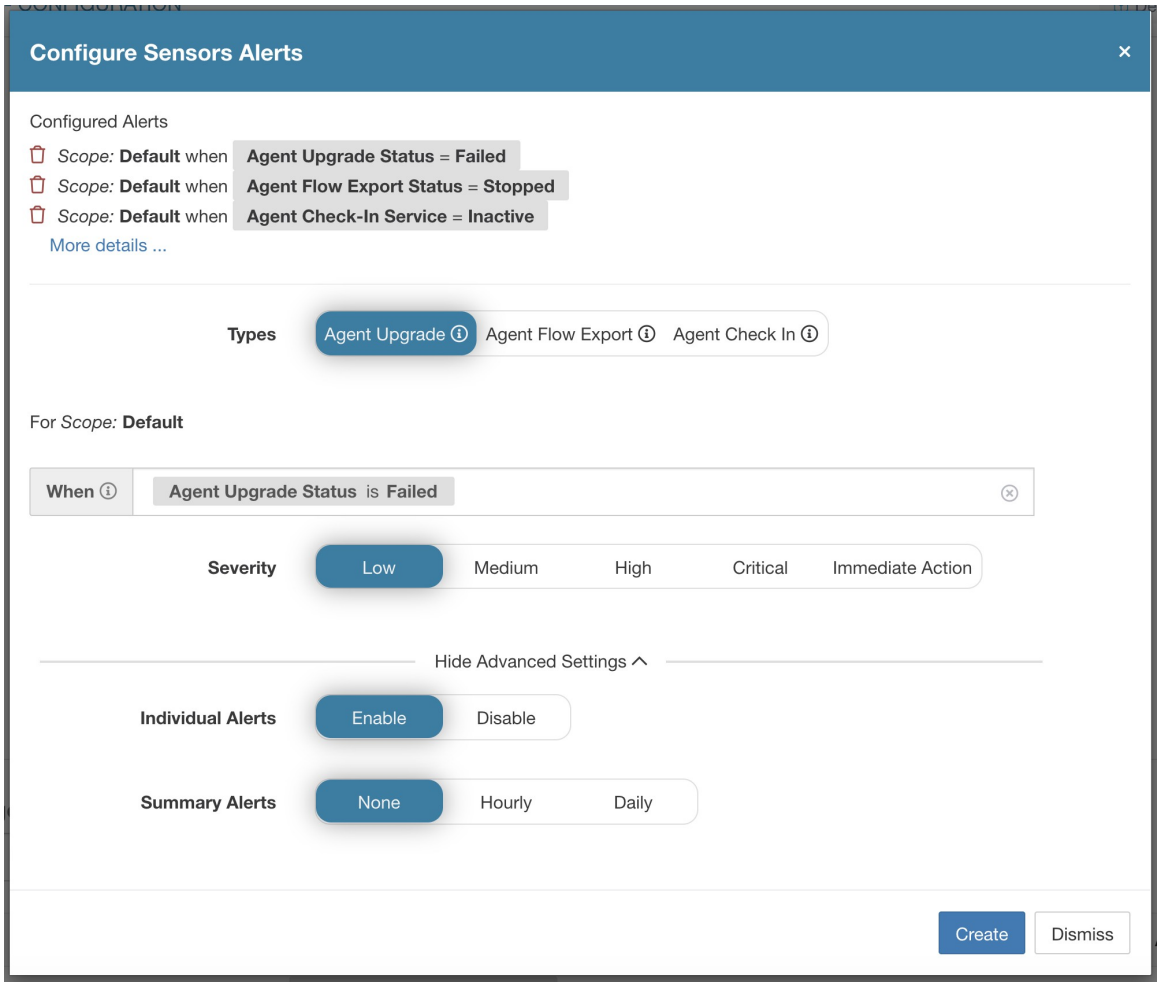
La configuration des alertes de capteur permet de configurer différents types d'alertes. Vous pouvez définir la gravité de l'alerte et les types de paramètres de configuration.

Pour en savoir plus, consultez Boîte de dialogue modale de configuration des alertes.

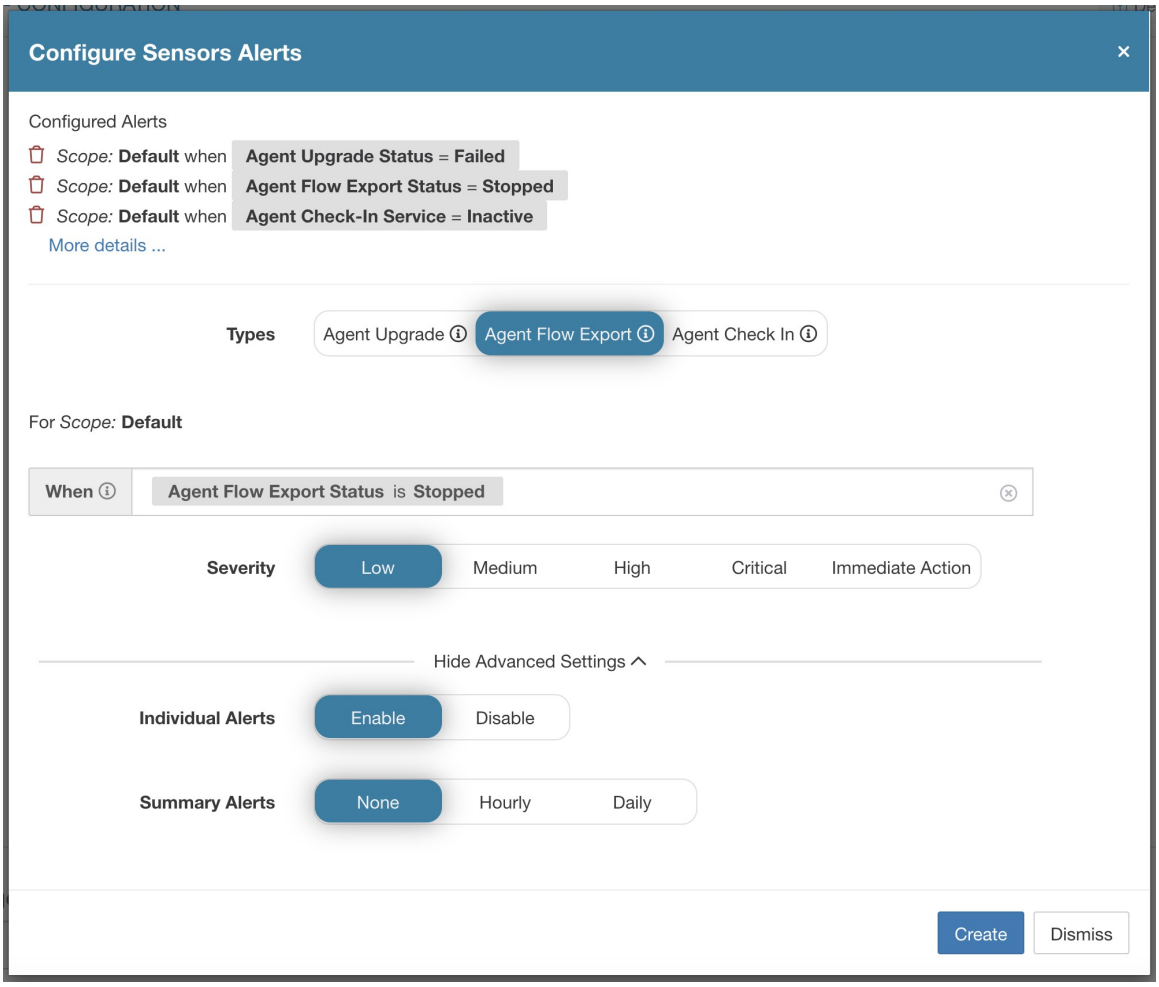
Note À partir de Cisco Secure Workload 3.5, vous pouvez configurer les alertes de capteur à l'aide du *modèle d'alerte de configuration*.

Figure 36: Configurer les alertes de capteur

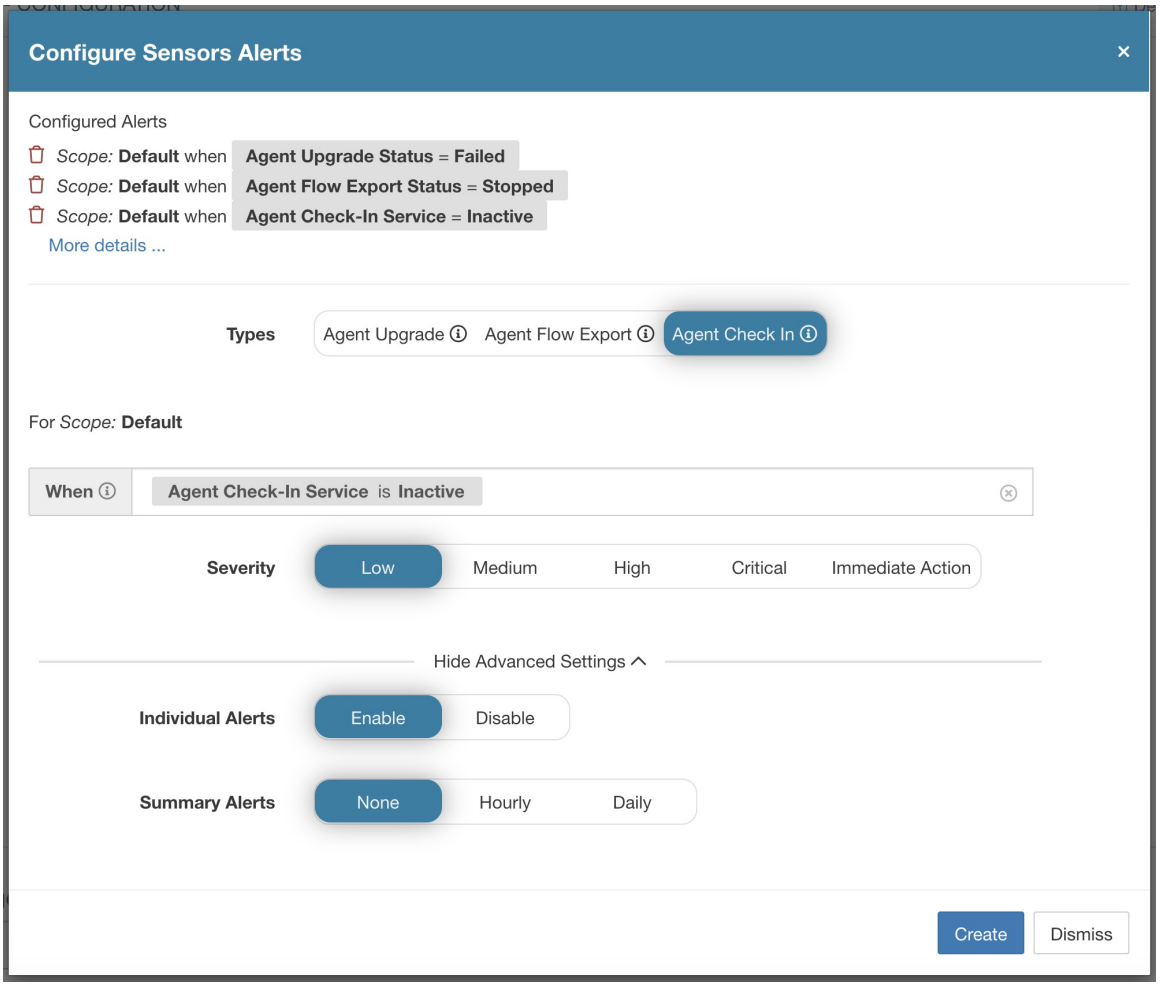




Configurer les alertes du capteur pour signaler l'échec de la mise à niveau d'un agent. Cette alerte se déclenche si l’agent n’a pas réussi à effectuer la mise à niveau vers la version nécessaire.



Configurer les alertes du capteur pour détecter quand l'exportation de flux d'agent doit s'arrêter. Cette alerte se déclenche si la connectivité est bloquée entre l'agent et la grappe, empêchant ainsi les flux et autres informations système d'être envoyées ou fournies.



Configurer les alertes des capteurs pour détecter l'expiration du délai de vérification de l'agent. Cette alerte se déclenche si la grappe ne reçoit pas de demande d'enregistrement d'un agent pendant plus de 90 minutes.

Figure 37: Configurer les alertes de capteur

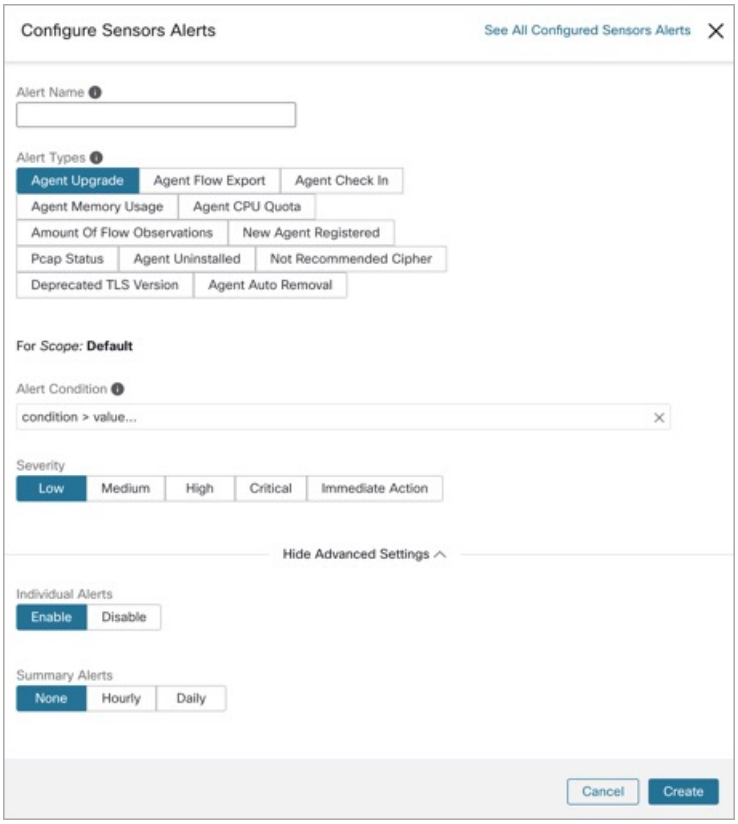


Figure 38: Configurer les alertes de capteur dans la configuration des alertes

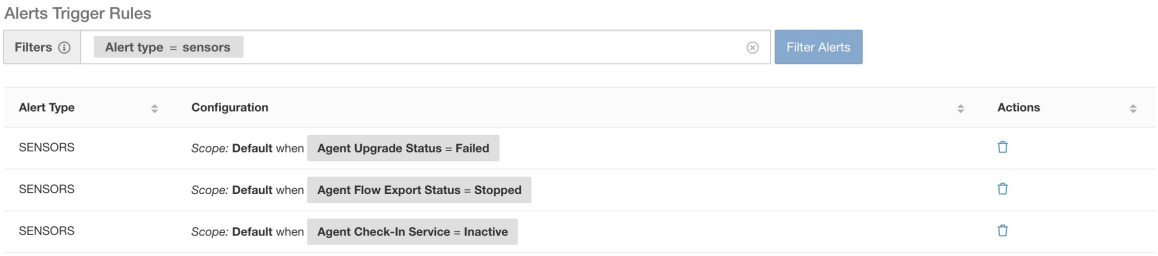
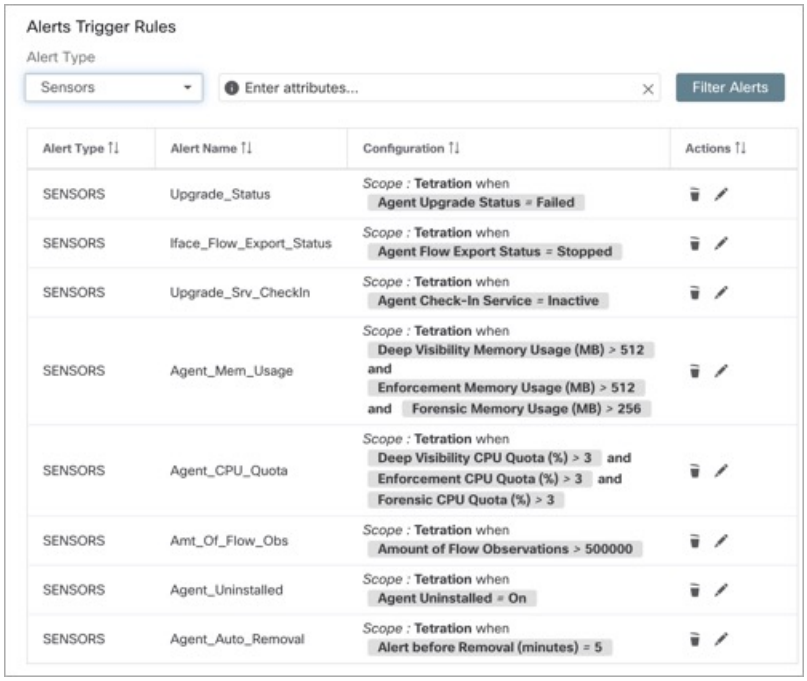
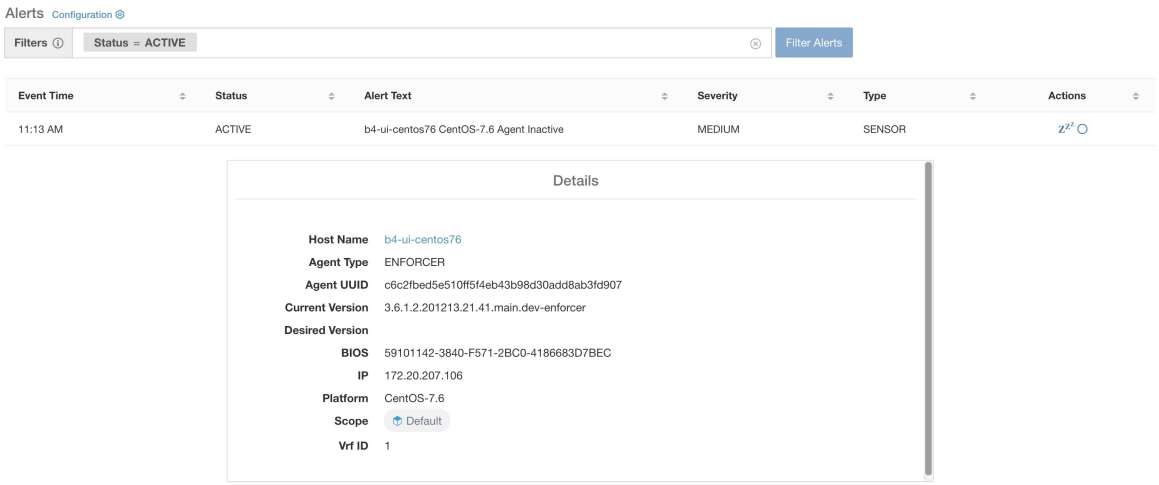


Figure 39: Afficher les alertes de capteur



Détails des alertes de l'interface utilisateur des capteurs

Figure 40: Alertes de capteurs



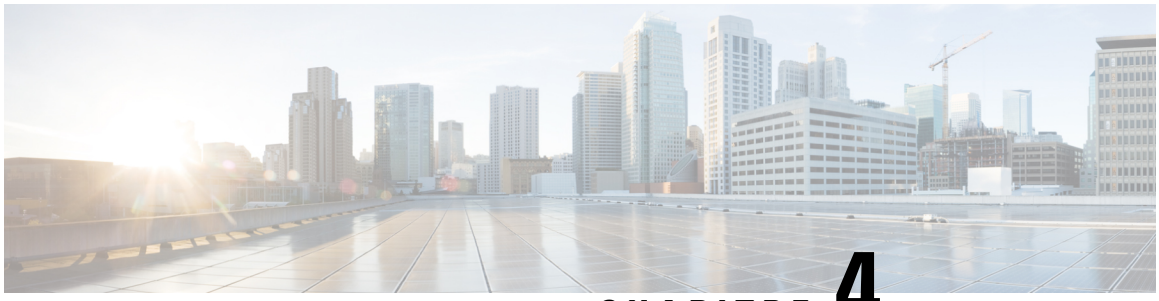
Détails de l'alerte de capteur

Pour connaître la structure générale des alertes et pour en savoir plus sur les champs, consultez la section Structure commune des alertes. Le champ *alert_détails* (détails des alertes) est structuré et contient les sous-champs suivants pour les alertes de capteurs

Champ	Type d'alerte	Format	Explication
Type d'agent	*tous*	chaîne	« ENFORCER » (APPLICATEUR) ou « SENSOR » (CAPTEUR) selon le type d'installation
Nom de l'hôte :	*tous*	chaîne	Nom de l'hôte sur lequel l'agent est déployé
IP	*tous*	chaîne	Adresse IP du nœud ou de la passerelle
Biographies	*tous*	chaîne	UUID BIOS du nœud
Observations	*tous*	chaîne	Renseignements sur la plateforme ou le système d'exploitation du nœud
Version actuelle	*tous*	chaîne	Version du logiciel de l'agent sur le nœud
Version souhaitée	*tous*	chaîne	Version du logiciel souhaitée pour l'agent
LastConfigFetchAt	*tous*	nombre entier	Horodatage Unix de la dernière fois que l'agent a envoyé une requête HTTPS

Exemple de détails_alertes pour une alerte de capteur


```
{
  "AgentType":"SENSOR",
  "Bios":"72EF1142-03A2-03BC-C2F8-F600567BA320",
  "CurrentVersion":"3.5.1.1.mrpm.build.win64-sensor",
  "DesiredVersion":"",
  "HostName":"win2k12-production-db",
  "IP":"172.26.231.193",
  "Platform":"MSServer2012R2Standard"
}
```



CHAPITRE 4

Orchestrateurs externes dans Cisco Secure Workload

Les orchestrateurs externes sont utilisés pour rassembler les métadonnées existantes décrivant vos charges de travail à partir des systèmes de votre réseau. Certains orchestrateurs externes peuvent également appliquer la politique de segmentation.

Pour les déploiements pour lesquels un système d'enregistrement autorisé avec des étiquettes pour les charges de travail existe, nous offrons un moyen d'importer automatiquement les étiquettes au moyen d'intégrations d'orchestrateurs externes. Toute modification dans le système d'enregistrement sera apprise automatiquement par Cisco Secure Workload et utilisée pour la mise à jour des étiquettes de votre inventaire.

Pour des renseignements détaillés sur la puissance et les utilisations des étiquettes, consultez Étiquettes de charge de travail.

En raison des récentes mises à jour de l'interface graphique, certaines images ou captures d'écran utilisées dans le guide de l'utilisateur peuvent ne pas refléter pleinement la conception actuelle du produit. Nous recommandons d'utiliser ce guide en conjonction avec la dernière version du logiciel pour obtenir la référence visuelle la plus précise.

Accéder à la page des orchestrateurs externes

La page principale pour les orchestrateurs externes est accessible en sélectionnant **Manage (Gestion)** > **Workloads(Charges de travail)** > **External Orchestrators (Orchestrateurs externes)** dans la barre de menus à gauche.

Liste des orchestrateurs externes

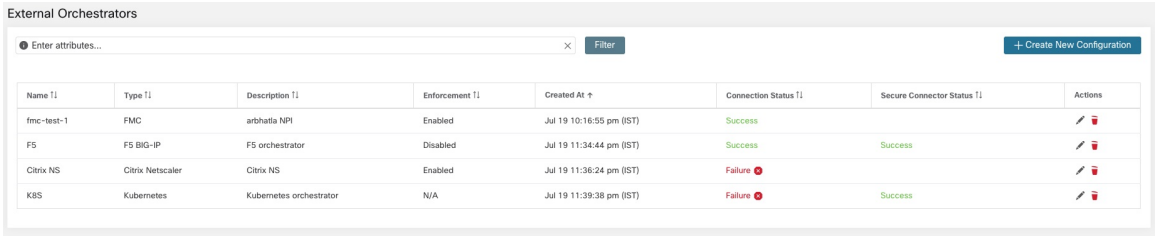
La page External Orchestrateurs (Orchestrateurs externes) affiche les orchestrateurs externes existants et fournit des fonctions pour les modifier et les supprimer ainsi que pour en créer de nouveaux :

Table 14: Orchestrateurs externes

Type	Description/Quand l'utiliser
VMware vCenter	Pour importer les données de la machine virtuelle, tels que le nom d'hôte, l'adresse IP et les étiquettes, d'un serveur vCenter vers Cisco Secure Workload. Les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.
Amazon Web Services	(Vous ne pouvez pas créer de nouveaux orchestrateurs AWS; créez plutôt des connecteurs AWS. Consultez la section Connecteur AWS. Tous les orchestrateurs AWS existants sont en lecture seule). Pour importer les données des instances de serveur EC2, telles que le nom d'hôte, l'adresse IP et les étiquettes, depuis le compte AWS vers Cisco Secure Workload. Les étiquettes générées sont utiles pour créer des portées et des politiques Cisco Secure Workload.
Kubernetes/OpenShift	Pour importer les entités de Kubernetes, telles que les nœuds, les pods, les services et les étiquettes. Ces étiquettes peuvent être utilisées au sein de Cisco Secure Workload pour définir des portées et des politiques.
DNS	Pour importer des enregistrements A/AAAA et CNAME à partir d'un serveur DNS par transfert de zone. Cela produit des noms DNS sous forme d'étiquettes, qui sont utiles pour définir les portées et les politiques Cisco Secure Workload.

Type	Description/Quand l'utiliser
Infoblox	Pour importer des réseaux, des hôtes et des enregistrements A/AAAA avec des attributs extensibles à partir d'un appareil Infoblox avec IPAM/DNS activé. Les attributs extensibles importés peuvent être utilisés comme étiquettes dans les portées et les politiques Cisco Secure Workload.
F5 BIG-IP	Pour lire les configurations de serveur virtuel à partir d'un équilibreur de charge F5 donné et générer des étiquettes pour les services fournis, qui peuvent être utilisés pour définir les politiques d'application dans Cisco Secure Workload. La fonction d'application de la politique les traduira en règles F5 à l'aide de l'API REST F5.
Citrix Netscaler	Pour lire les configurations de serveur virtuel à partir d'un équilibreur de charge Netscaler donné et générer des étiquettes pour les services fournis, qui peuvent être utilisés pour définir des politiques d'application dans Cisco Secure Workload. La fonctionnalité d'application des politiques les traduira en ACL Netscaler via son API REST.
Cisco Secure Firewall Management Center	Pour déployer les politiques sur tous les périphériques Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense ou FTD) enregistrés sur Cisco Secure Firewall Management Center à l'aide de l'API REST.

Figure 41: Orchestrateur externe

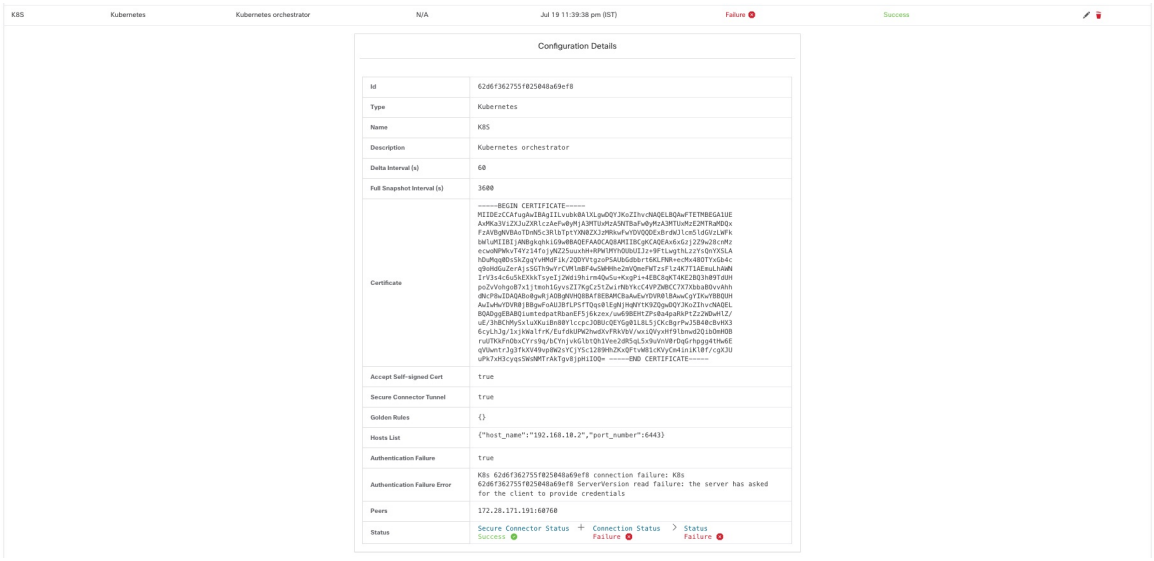


Chaque ligne affiche une version abrégée de l'orchestrateur externe comportant son *nom*, son *type*, sa *description*, son *application*, son statut *Créé à*, l'état de *la connexion* et l'*état du connecteur sécurisé Secure Connector*. L'état de la connexion indique si une connexion à une source de données externe a pu être établie avec succès. *Secure Connector Status* (État du connecteur sécurisé) affiche l'état du tunnel Secure Connector (succès ou échec). Si le tunnel n'est pas activé, N/A s'affiche.

Activez le tunnel du connecteur sécurisé lors de la création d'une configuration d'orchestrateur externe. Si le tunnel de connecteur sécurisé est activé, « l'état de la connexion » de l'orchestrateur externe dépend à la fois de l'état d'authentification et de l'état du connecteur sécurisé. Si le tunnel du connecteur sécurisé n'est pas activé, « l'état de la connexion » de l'orchestrateur externe dépend uniquement de l'état d'authentification. Quel que soit l'état (réussite ou échec), vous pouvez cliquer sur la ligne respective pour obtenir plus de détails.

Pour plus de détails sur les mesures du client du connecteur sécurisé, cliquez sur la ligne **Status** (État) ou, dans le volet gauche, accédez à **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (connecteur sécurisé)**.

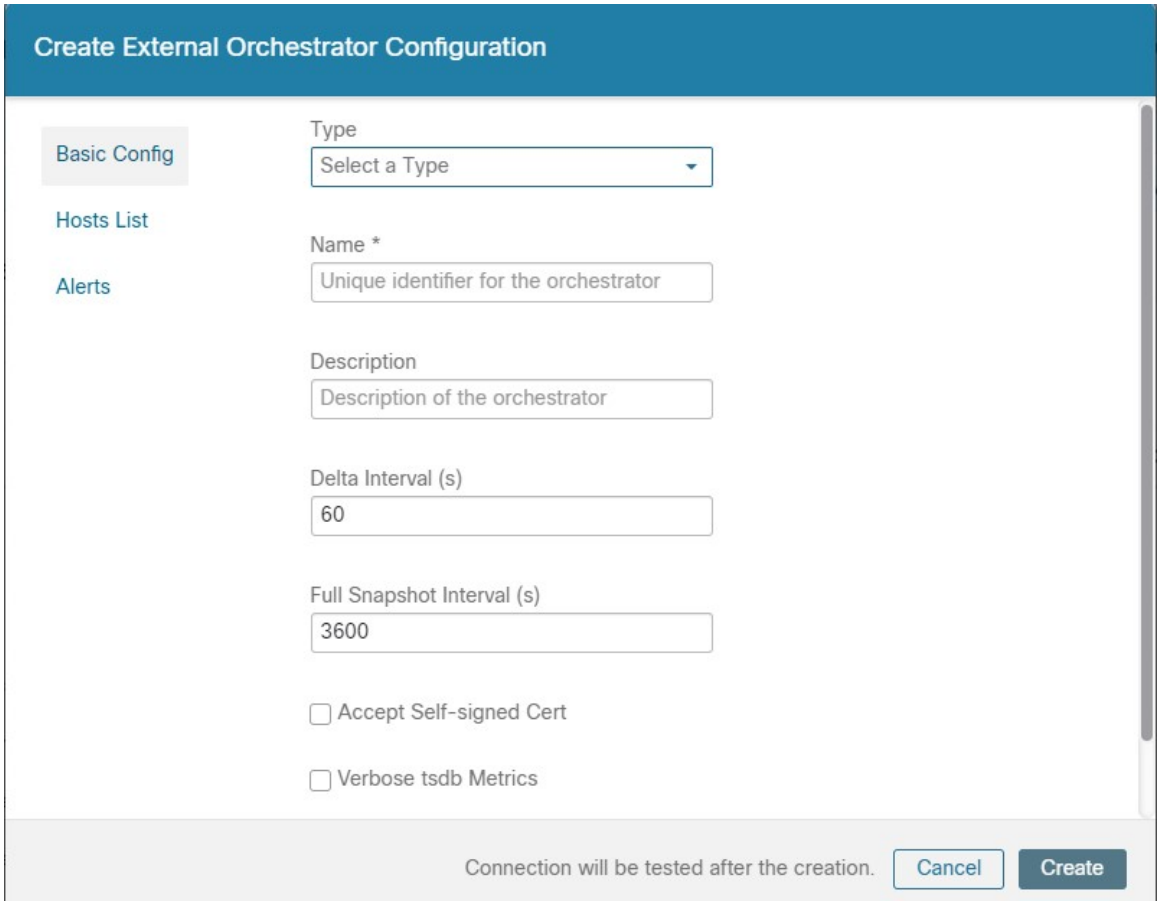
Figure 42: Échec de l'authentification de l'orchestrateur externe



Créer un orchestrateur externe

Un orchestrateur externe peut être créé en cliquant sur le bouton **Create New Configuration** (Créer une nouvelle configuration) dans la page principale des orchestrateurs externes. Une boîte de dialogue modale s'ouvre, dans laquelle vous pouvez saisir un nom et choisir un type d'orchestrateur externe. L'image ci-dessous montre la page de configuration de base :

Figure 43: Créer une configuration d'orchestrateur externe



Le tableau suivant décrit les champs communs aux orchestrateurs externes. Selon le type sélectionné, la page de *configuration de base* nécessite la saisie de paramètres supplémentaires. Ceux-ci seront couverts par la section respective des orchestrateurs externes individuels ci-dessous.

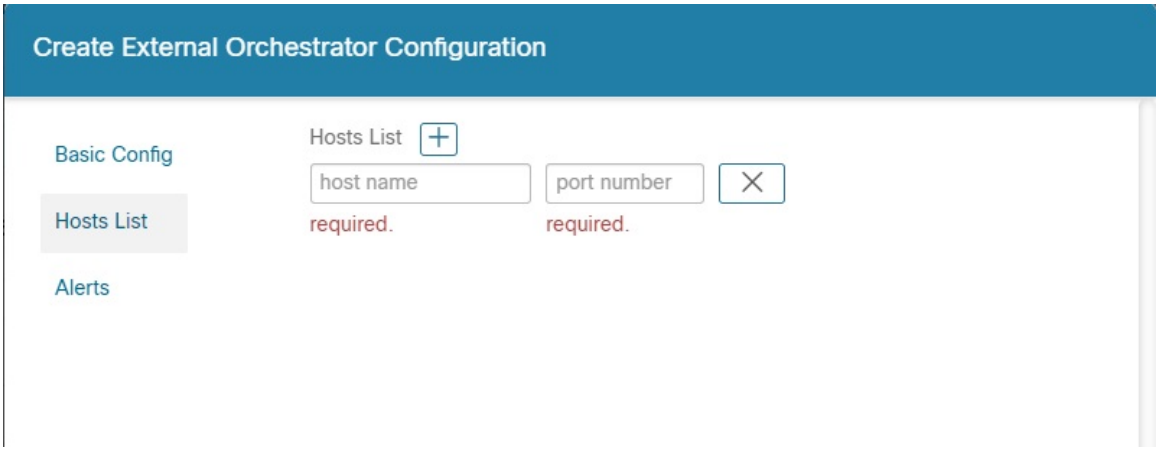
Champs communs	Obligatoire	Description
Type	Oui	Sélectionnez un orchestrateur externe dans la liste.
Nom	Oui	Nom de l'orchestrateur externe, qui doit être unique pour le détenteur actif.
Description	Non	Description de l'orchestrateur externe.
Intervalle(s) complet(s) de l'instantané	Oui	Intervalle en secondes pendant lequel l'orchestrateur externe tentera d'importer l'instantané complet de la configuration à partir du *Type* sélectionné.

Champs communs	Obligatoire	Description
Accept Self-signed Cert (Accepter le certificat autosigné)	Non	Cochez cette option pour accepter les certificats de serveur autosignés pour la connexion HTTPS utilisée par Cisco Secure Workload afin de récupérer les données de configuration du *Type*. Par défaut, les certificats de serveur autosignés ne sont pas autorisés.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Non	Cochez cette option pour définir les connexions à la grappe Cisco Secure Workload pour qu'elles soient acheminées par un tunnel de connecteur sécurisé.

Note Les champs *Intervalle différentiel* et *Mesures TSDB détaillées* , comme le montre l'image ci-dessus sont facultatifs et applicables uniquement à certains orchestrateurs externes, qui sont présentés dans les descriptions respectives ci-dessous.

À l'exception du type d'orchestrateur externe *AWS*, la *Hosts List* (Liste des hôtes) doit être fournie. Elle spécifie les adresses réseau de la source de données externe à partir de laquelle l'orchestrateur externe récupérera les données et générera des étiquettes. Pour ce faire, cliquez sur l'onglet *Hosts List* (liste des hôtes) sur le côté gauche, comme le montre l'image suivante :

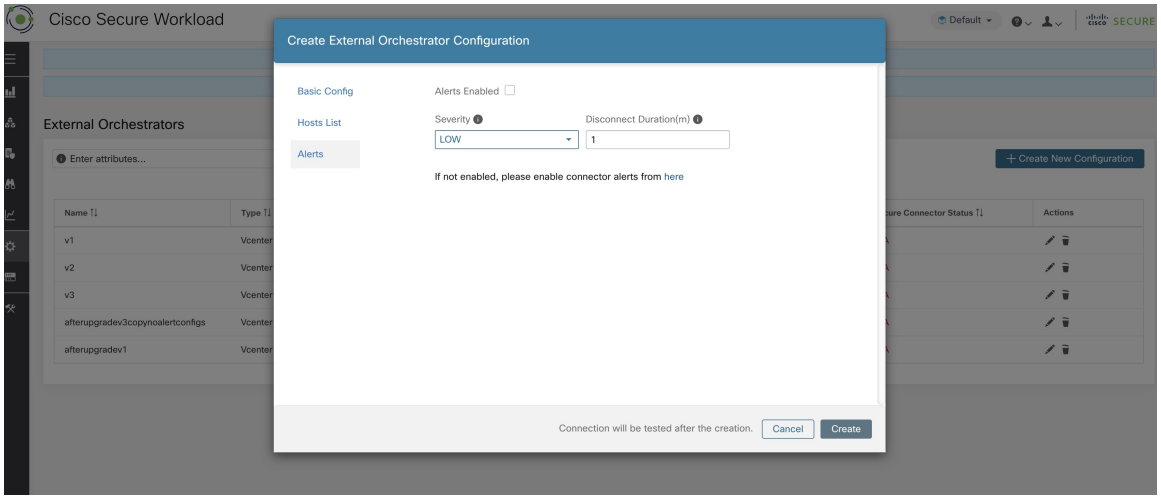
Figure 44: Liste des hôtes de l'orchestrateur externe



Pour ajouter une nouvelle entrée à la liste d'hôtes, cliquez sur le signe plus. Chaque ligne doit contenir un nom d'hôte DNS valide, une adresse IPv4 ou IPv6 et un numéro de port. Selon le type d'orchestrateur externe choisi, vous pouvez saisir plusieurs hôtes à des fins de haute disponibilité ou de redondance. Pour en savoir plus, consultez la description de l'orchestrateur externe choisi.

Pour définir l'alerte pour l'orchestrateur externe, vous pouvez le faire en cliquant sur l'onglet *Alerte* sur le côté gauche, comme le montre l'image suivante :

Figure 45: Alertes de l'orchestrateur externe



Pour chaque orchestrateur externe, la configuration des *alertes* nécessite que des paramètres supplémentaires soient fournis. Ceux-ci seront couverts par la section respective des orchestrateurs externes individuels ci-dessous.

Pour activer les alertes pour cet orchestrateur externe, cochez la case *Alert Enabled* (alerte activée).

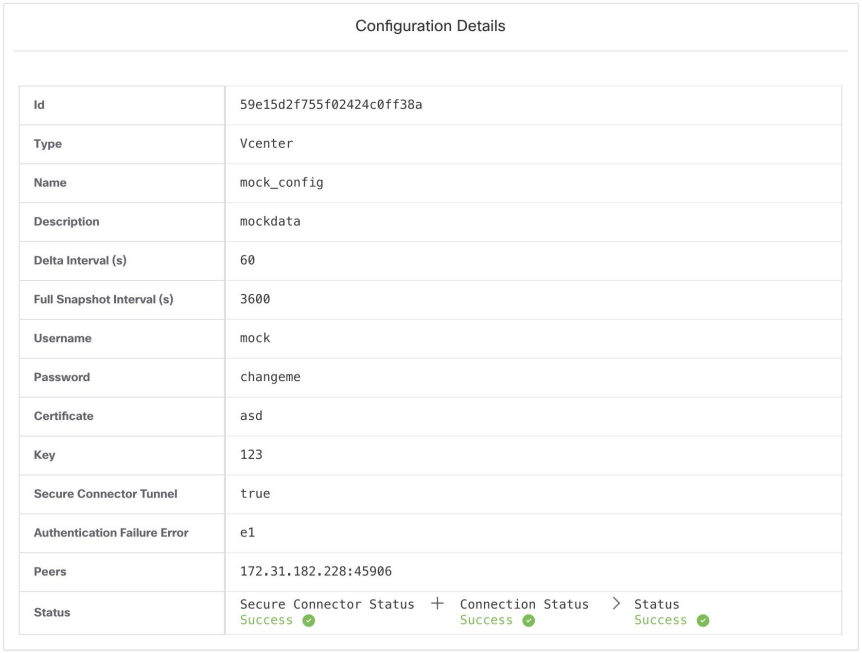
Note Assurez-vous que les alertes du connecteur sont également activées sur la page **Manage** > **Workloads** > **Alert Configs** (gestion des configurations d'alertes des charges de travail).

Sélectionnez le niveau de *Alert Severity* (gravité de l'alerte) et la *Disconnect Duration* (durée de la déconnexion) en minutes pour la configuration de l'alerte de l'orchestrateur externe.

Champ	Description
Gravité	Sélectionnez le niveau de gravité de cette règle :**LOW** (faible), **MEDIUM** (moyenne), **HIGH** (élevée), **CRITICAL** (critique) ou **IMMEDIATE ACTION** (Action immédiate)
Durée de la déconnexion (m)	La durée pendant laquelle une connexion est déconnectée.

Cliquez sur le bouton **Create** (créer) pour créer le nouvel orchestrateur externe, dont les détails de configuration peuvent être consultés en cliquant sur la ligne correspondante dans la vue de liste :

Figure 46: Détails de la configuration de l'orchestrateur externe

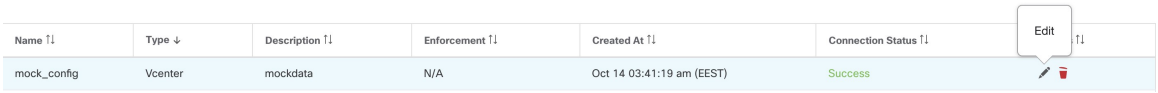


Note Étant donné que la première récupération complète d'instantané à partir d'un orchestrateur externe est une opération asynchrone, comptez environ une minute pour que le champ d'état de la connexion soit mis à jour.

Modifier un orchestrateur externe

Cliquez sur le bouton en forme de crayon à droite d'une ligne d'un orchestrateur externe, comme illustré ci-dessous, pour ouvrir une boîte de dialogue modale similaire à celle utilisée pour la création d'un orchestrateur externe, où la configuration peut être modifiée.

Figure 47: Modifier un orchestrateur externe



Note

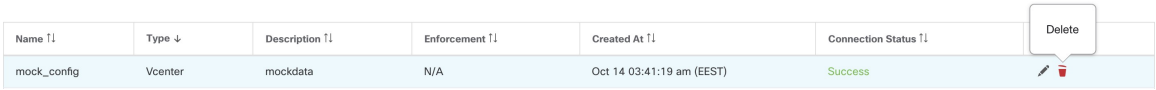
- Le champ **Type** n'est pas modifiable.
- Si une configuration utilise des clés ou des certificats pour l'authentification, les clés et les certificats doivent être fournis à chaque mise à jour de la configuration.
- Étant donné que les modifications de configuration d'un orchestrateur externe est réalisée de manière asynchrone, comptez environ une minute pour que le champ d'état de la connexion soit mis à jour et pour confirmer l'exactitude des modifications saisies.

Cliquez sur le bouton **Update** (mettre à jour) pour enregistrer les modifications apportées à la configuration.

Supprimer un orchestrateur externe

Caution La suppression d'un orchestrateur externe entraîne également la suppression des étiquettes fournies par cet orchestrateur, ce qui aura une incidence sur les politiques. Pour supprimer un orchestrateur externe, cliquez sur la corbeille comme indiqué ci-dessous :

Figure 48: Supprimer un orchestrateur externe



Étiquettes générées par l'orchestrateur

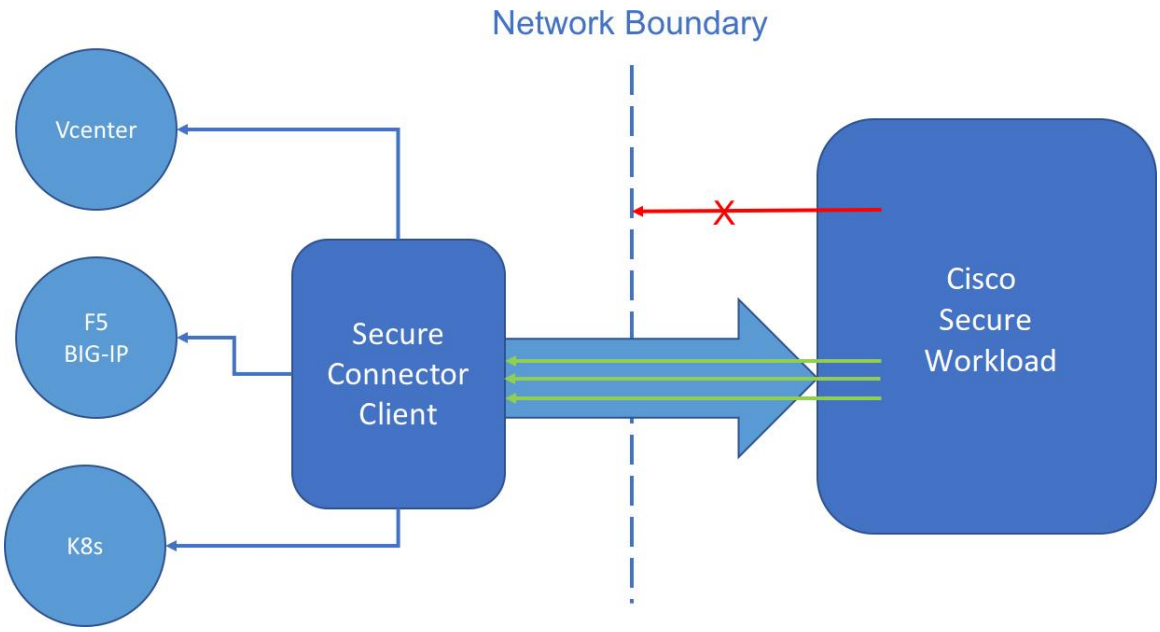
Cisco Secure Workload ajoute les étiquettes suivantes à toutes les instances AWS.

Clé	Valeur
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	*<Nom de la grappe Kubernetes>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/cluster_id	*<UUID de la configuration de l'orchestrateur dans |produit|>*

Connecteur sécurisé

Pour que Cisco Secure Workload puisse importer des balises utilisateur ou appliquer des politiques sur les orchestrateurs externes (voir Orchestrateurs externes dans Cisco Secure Workload), Cisco Secure Workload doit établir des connexions sortantes vers les serveurs d'API des orchestrateurs (vCenter, Kubernetes, F5 BIG-IP, etc.). Parfois, il n'est pas possible d'autoriser les connexions entrantes directes vers les orchestrateurs à partir de la grappe Cisco Secure Workload. Le connecteur sécurisé résout ce problème en établissant une connexion sortante du même réseau que l'orchestrateur vers la grappe Cisco Secure Workload. Cette connexion est utilisée comme tunnel inverse pour renvoyer les demandes de la grappe au serveur d'API de l'orchestrateur.

Figure 49: Connecteur sécurisé



Pour chaque portée racine, un seul tunnel à la fois peut être actif. Les tentatives de démarrage de tunnels supplémentaires seront rejetées avec un message d'erreur indiquant qu'un tunnel est déjà actif. Le tunnel actif peut être utilisé pour se connecter à plusieurs orchestrateurs qui sont accessibles à partir du réseau dans lequel le client fonctionne. Une configuration par orchestrateur est utilisée pour indiquer si les connexions à cet orchestrateur doivent passer par le tunnel du connecteur sécurisé.

Toutes les communications entre le client Connecteur sécurisé et la grappe Cisco Secure Workload sont authentifiées et chiffrées mutuellement à l'aide de TLS.

Pour une sécurité accrue, il est conseillé aux clients d'installer le client Secure Connector (Connecteur sécurisé) sur un ordinateur isolé correctement sécurisé. L'ordinateur doit avoir des règles de pare-feu pour autoriser les connexions sortantes uniquement vers la grappe Cisco Secure Workload et tous les serveurs API externes de l'orchestrateur Cisco Secure Workload doivent être autorisés à y accéder.

Pour configurer les orchestrateurs en vue de l'utilisation du tunnel du connecteur sécurisé, consultez les instructions de configuration de l'orchestrateur externe pour votre produit.

Pour en savoir plus sur les points terminaux OpenAPI pour le connecteur sécurisé, consultez : Points d'accès d'API du connecteur sécurisé

Détails techniques

Pour amorcer le tunnel, le client connecteur sécurisé crée une paire de clés publique ou privée et signe son certificat de clé publique à distance par le serveur. Un jeton cryptographique à usage unique d'une durée limitée est utilisé pour sécuriser ce processus de signature à distance et pour identifier la portée racine à laquelle le client appartient. Du côté du serveur, chaque portée racine possède un certificat unique que le client utilise pour authentifier le serveur. Ces certificats sont régulièrement renouvelés pour assurer le secret de communication.

Le client connecteur sécurisé est composé d'un client de tunnel et d'un serveur SOCKS5. Une fois le tunnel démarré, le client attend les connexions par tunnellisation entrantes de la grappe Cisco Secure Workload. Les connexions entrantes sont gérées par le serveur SOCKS5 et transférées à l'hôte de destination.

Exigences relatives au client Connecteur sécurisé

Voici les exigences pour le client Connecteur sécurisé :

- RHEL ou CentOS 7 (x86_64)
- 2 cœurs de CPU
- 4 Go de RAM
- Une bande passante réseau suffisante pour gérer les données des orchestrateurs sur site qui utilisent le connecteur sécurisé.
- Connectivité sortante vers la grappe Cisco Secure Workload sur le port 443 (directe ou par l'intermédiaire d'un serveur mandataire HTTP(S)).
- Connectivité sortante vers les serveurs d'API Orchestrator internes (directe)

Déploiement client du connecteur sécurisé

Prise en charge de serveur mandataire

Le client du connecteur sécurisé prend en charge la connexion à la grappe Cisco Secure Workload par l'intermédiaire d'un serveur mandataire HTTP(S). Au besoin, le serveur mandataire doit être configuré en définissant la variable d'environnement HTTPS_PROXY pour le client. Pour définir la variable, ajoutez la ligne suivante dans la section *[Service]* du fichier de service systemd situé à l'emplacement */etc/systemd/system/tetration- secure-connector.service*. Ce paramètre ne sera pas conservé lors des réinstallations. Pour une configuration permanente, la ligne peut être ajoutée dans un nouveau fichier à l'adresse suivante */etc/systemd/system/tetration-secure-connector.service.d/10-https-proxy.conf*. Pour que l'une ou l'autre des configurations prenne effet, rechargez la configuration systemd en exécutant *systemctl daemon-reload*.

```
[Service]
Environment="HTTPS_PROXY=<Proxy Server Address>"
```

Présentation du déploiement

Le connecteur sécurisé crée un tunnel inverse de la grappe Cisco Secure Workload à votre réseau interne afin d'atteindre les serveurs d'API de votre orchestrateur.

Le démarrage du client du connecteur sécurisé nécessite le téléchargement du RPM Secure Connector et la génération d'un jeton d'enregistrement à usage unique.

1. Télécharger le dernier RPM du client du connecteur sécurisé sur une plateforme prise en charge.
2. Générer un jeton d'enregistrement.
3. Copier le jeton et démarrer le client sur l'hôte pour démarrer le client.

Déployer le client connecteur sécurisé

Télécharger le dernier RPM du client du connecteur sécurisé

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

Étape 2 Cliquez sur **Download Latest RPM** (Télécharger le dernier RPM).

Étape 3 Copiez l'ensemble RPM sur l'hôte Linux pour le déploiement, puis exécutez la commande suivante avec les privilèges racine :`rpm -ivh <rpm_filename>`.

Générer un jeton d'enregistrement

Procédure

Étape 1 Cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

Étape 2 Cliquez sur **Generate Registration Token** (Générer un jeton d'enregistrement).

Copier le jeton et démarrer le client

Après avoir généré un jeton d'enregistrement sur la page **Secure Connector** (connecteur sécurisé), vous obtiendrez un fichier *registration.token* (jeton d'enregistrement) qui contient le jeton à usage unique à durée limitée pour le démarrage du client. Arrêtez le client connecteur sécurisé sur l'hôte et copiez le fichier de jeton à l'emplacement où vous avez installé le paquet client connecteur sécurisé.

1. Pour arrêter le client, exécutez la commande suivante : `systemctl stop tetration-secure-connector`
2. Copiez le fichier *registration.token* dans le dossier `/etc/tetration/cert/`.
3. Pour redémarrer le client, exécutez la commande suivante : `systemctl start tetration-secure-connector`

[Facultatif] Déployer la version spécifique du client connecteur sécurisé

Procédure

Étape 1 Téléchargez une version précise du client connecteur sécurisé RPM.

a) Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)**.
b) Cliquez sur l'onglet **Installer** (Programme d' installation).
c) Cliquez sur **Manual Install using classic packaged installers (Installation manuelle à l'aide des programmes d'installation classiques)**, puis cliquez sur **Next**(suivant).

Les progiciels client connecteur sécurisé ont le type d'agent *Secure Connector* (Connecteur sécurisé).

d) Recherchez la version appropriée (si plusieurs sont disponibles sur la grappe) et cliquez sur **Download** (Télécharger).

e) Copiez l'ensemble RPM sur l'hôte Linux pour le déploiement, puis exécutez la commande suivante avec les privilèges racine :`rpm -ivh <rpm_filename>`.

Étape 2 Récupérez un nouveau jeton à l'aide de l'API.

Les jetons du connecteur sécurisé peuvent également être récupérés par le biais de l'OpenAPI (Obtenir un jeton). Les extraits de code Python et Bash suivants peuvent être utilisés pour récupérer un nouveau jeton. Notez que la clé API utilisée doit avoir la capacité *external_integration* et avoir un accès en écriture à la portée racine spécifiée. Consultez la section Authentification OpenAPI (Authentification OpenAPI) pour obtenir des renseignements sur l'installation de OpenAPI client Cisco Secure Workload pour Python et la création d'une nouvelle clé API.

- **Fragment de code Python pour la récupération de jetons**

```
from tetpyclient import RestClient
from urllib import quote

API_ENDPOINT = "https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
ROOT_SCOPE_NAME = r"""<ROOT_SCOPE_NAME>"""
API_CREDENTIALS_FILE = "<API_CREDENTIALS_JSON_FILE>"
OUTPUT_TOKEN_FILE = "registration.token"

if __name__ == "__main__":
  client = RestClient(API_ENDPOINT,
                      credentials_file=API_CREDENTIALS_FILE)  # Add (verify=False) to
skip certificate verification
  escaped_root_scope_name = quote(ROOT_SCOPE_NAME, safe='')
  resp = client.get('/secureconnector/name/{}/token'.format(escaped_root_scope_name))
  if resp.status_code != 200:
    print 'Error ({}): {}'.format(resp.status_code, resp.content)
    exit(1)
  else:
    with open(OUTPUT_TOKEN_FILE, 'w') as f:
      f.write(resp.content)
```

- **Fragment de code BASH pour la récupération de jetons**

```
#!/bin/bash
HOST="https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
API_KEY="<API_KEY>"
API_SECRET="<API_SECRET>"
ROOTSCOPE_NAME="<ROOT_SCOPE_NAME>" # if the name contains spaces or special characters,
 it should be url-encoded
TOKEN_FILE="registration.token"
INSECURE=1 # Set to 0 if you want curl to verify the identity of the cluster

METHOD="GET"
URI="/openapi/v1/secureconnector/name/$ROOTSCOPE_NAME/token"
CHK_SUM=""
CONTENT_TYPE=""
TS=$(date -u "+%Y-%m-%dT%H:%M:%S+0000")
CURL_ARGS="-v"
if [ $INSECURE -eq 1 ]; then
    CURL_ARGS=$CURL_ARGS" -k"
fi
```

```
    MSG=$(echo -n -e "$METHOD\n$URI\n$CHK_SUM\n$CONTENT_TYPE\n$TS\n")
   SIG=$(echo "$MSG"| openssl dgst -sha256 -hmac $API_SECRET -binary | openssl enc -base64)

    REQ=$(echo -n "curl $CURL_ARGS $HOST$URI -w '%{http_code}' -H 'Timestamp: $TS' -H 'Id:
$API_KEY' -H 'Authorization: $SIG' -o $TOKEN_FILE")
    status_code=$(sh -c "$REQ")
    if [ $status_code -ne 200 ]; then
        echo "Failed to get token. Status: " $status_code
    else
        echo "Token retrieved successfully"
    fi
```

Étape 3 Copier le jeton et démarrer le client. Pour plus de renseignements sur les instructions, consultez Copier le jeton et démarrer le client, à la page 136.

Vérifier l'état du client connecteur sécurisé

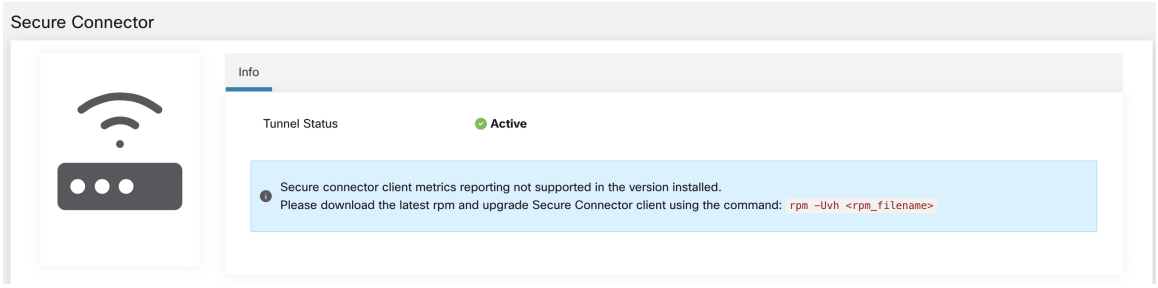
- Pour vérifier si le client Connecteur sécurisé est installé, interrogez la base de données RPM pour trouver le paquet *tet- secureconnector-client-site* en exécutant la commande suivante : `rpm -q tet-secureconnector-client-site`
- Pour vérifier l'état du client installé, vous pouvez vérifier l'état du service *tetration-secure-connector* systemd en exécutant la commande suivante : `systemctl status tetration-secure-connector`

État du client du connecteur sécurisé

Dans la page **External Orchestrateurs**, l'état des orchestrateurs externes configurés et du tunnel du connecteur sécurisé s'affiche. Si le connecteur sécurisé est activé lors de la configuration des orchestrateurs externes, vous pouvez afficher les métriques du client **Secure Connector** dans la page Secure Connector (connecteur sécurisé).

Cependant, si l'état du tunnel de Cisco Secure Connector est **Actif** mais que les métriques du client ne sont pas visibles, cela signifie qu'une version plus ancienne de Cisco Secure Connector est installée. Un message de mise à niveau dans la version de Secure Connector Client s'affiche comme suit :

Figure 50: Message de mise à niveau du client de connecteur sécurisé



Note Pour obtenir des instructions sur l'installation du dernier RPM client du connecteur sécurisé, consultez la section Télécharger le dernier RPM du client du connecteur sécurisé.

Pour afficher les mesures du client :

Procedure

Étape 1 Sous **Configure Details**(Détails de la configuration), cliquez sur la ligne **Status** (État). La page **Secure Connector** (Connecteur sécurisé) s'affiche.

Note Pour accéder à l'état du tunnel Secure Connector, sélectionnez **Manage(Gestion)** > **Workloads (Charges de travail)** > **Secure Connector(Connecteur sécurisé)** dans le volet gauche.

Étape 2 Sélectionnez les onglets **General**(General), **Interface**(Interface) ou **Routes** (routes) pour accéder à plus de détails sur l'état de la connectivité entre le client et la grappe Cisco Secure Workload.

Onglets	Description
Généralités	Répertorie les informations suivantes : • État du tunnel • Nom d'hôte • Adresse IP • Mandataire HTTP/HTTPS • Version : répertorie la version du build. • Nb de vCPU • Mémoire totale (Go) • Disponibilité : répertorie la disponibilité de la machine virtuelle sur laquelle le client du connecteur sécurisé est exécuté. • Last heartbeat Received (dernière pulsation reçue) : indique le jour et l'horodatage de la dernière pulsation reçue du client. • Nb d'échecs de pulsation (dernier jour) : indique le nombre d'échecs de la connectivité au client connecteur sécurisé au cours de la journée. Si le client reste inactif, le nombre n'est pas incrémenté. Le compte est réinitialisé à la fin de la journée. • Latence aller-retour (ms)
Interface	Répertorie les détails de l'interface de la machine virtuelle sur laquelle le client connecteur sécurisé est exécuté.

Onglets	Description
Routes	La table de routage répertorie les adresses IP de destination, la passerelle, le masque de génération et l'interface.

Alertes du connecteur sécurisé

L'alerte est générée lorsque le connecteur sécurisé cesse de fonctionner ou en l'absence de pulsation au cours de la dernière minute.

Étape 1 : pour activer l'alerte, cliquez sur **Manage (Gestion)** » **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

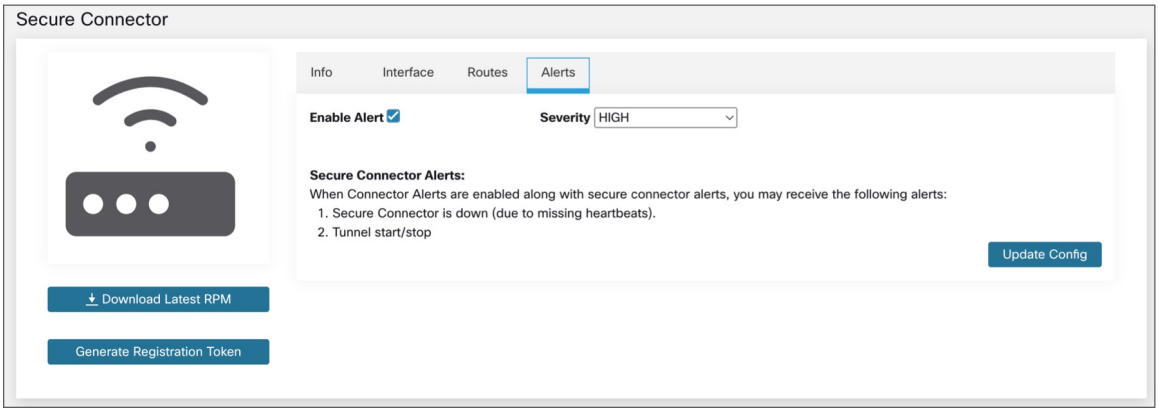
Étape 2 : cliquez sur l'onglet **Alerts** (alertes).

Étape 3 : Cochez la case **Enable Alert** (activer l'alerte).

Étape 4 : choisissez une valeur de **Severity** (gravité) dans le menu déroulant.

Étape 5 : Cliquez sur **Update Config** (Mettre à jour la configuration).

Illustration 51 : Activer les alertes du connecteur sécurisé



Remarque Assurez-vous que les alertes des connecteurs sont activées dans la page **Manage (Gestion)** > **Alerts - Configuration Configuration des alertes)**.

Accédez à **Investigate** (Enquêter) > **Alerts** (Alertes) et cliquez sur une alerte pour en savoir plus.

Texte d'alerte : : Secure Connector(connecteur sécurisé) : <motif de l'échec de la connexion>

Illustration 52 : Alerte du connecteur sécurisé

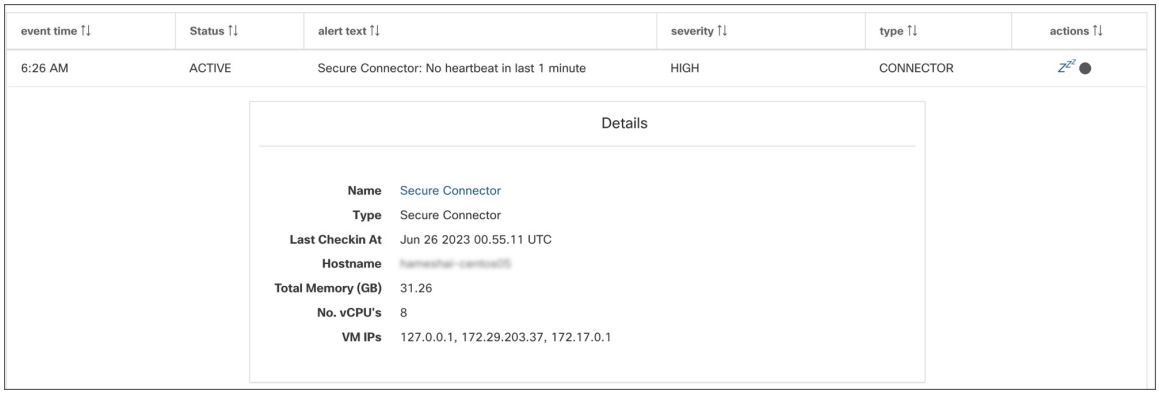


Tableau 15 : Détails de l'alerte

Champ	Type	Description
Nom	Chaîne	Nom du connecteur sécurisé
Type	Chaîne	Type du connecteur sécurisé
Last Checkin At	Chaîne	Dernière heure connue de pulsation
Hostname (Nom d'hôte)	Chaîne	Nom de la machine hébergeant ce connecteur sécurisé
Total Memory (GB)	Chaîne	RAM en Go
No. vCPU's	Chaîne	Nombre de CPU
VM IPs	Chaîne	Liste des interfaces réseau sur l'hôte client du connecteur sécurisé

Mettre à niveau le client connecteur sécurisé

Le client Secure Connector (Connecteur sécurisé) ne prend pas en charge les mises à jour automatiques. Pour déployer une nouvelle version :

1. Exécutez la commande suivante pour désinstaller la version actuelle : `rpm -e tet-secureconnector-client-site`
2. Déployez la nouvelle version. Pour plus de renseignements sur les instructions, consultez Déployer le client connecteur sécurisé, on page 136.

Désinstaller le client connecteur sécurisé

Le client connecteur sécurisé peut être désinstallé à l'aide de la commande suivante `rpm -e tet-secureconnector-client-site`

Amazon Web Services

Note La fonctionnalité d'orchestrateur externe d'AWS fait désormais partie de la nouvelle fonctionnalité de connecteur infonuagique AWS. Si vous avez effectué une mise à niveau vers cette version, vos orchestrateurs externes AWS existants sont maintenant en lecture seule; si vous devez apporter des modifications, créez un nouveau connecteur AWS. Pour en savoir plus, consultez Connecteur AWS.

Cisco Secure Workload prend en charge l'acquisition automatisée de l'inventaire en direct à partir d'une région AWS. Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « aws », l'appareil Cisco Secure Workload se connecte au point terminal AWS et récupère les métadonnées pour toutes les instances à l'état d'exécution ou d'arrêt.

Prérequis

- Les jetons de sécurité (clé d'accès et clé secrète) utilisés doivent avoir le type de privilèges IAM approprié pour permettre la récupération des informations de l'orchestrateur.

Champs de configuration

Attribut	Description
Identifiant	Identifiant unique de l'orchestrateur.
Nom	Nom spécifié par l'utilisateur de l'orchestrateur.
Type	Type d'orchestrateur - (*aws* dans ce cas)
Description	Une brève description de l'orchestrateur.
ID de la clé d'accès AWS	CLÉ D'ACCÈS associée au compte pour lequel la configuration de l'orchestrateur est en cours de création.
Clé d'accès secrète AWS	CLÉ SECRÈTE associée au compte que vous créez pour la configuration de l'orchestrateur. **Note** Saisissez à nouveau la clé secrète si vous modifiez la configuration de l'orchestrateur.
Région AWS	La région dans laquelle la charge de travail a été déployée. Si une charge de travail est répartie sur plusieurs régions, une configuration distincte est requise pour chaque région. Consultez le lien ci-dessous pour connaître les valeurs de *région* correctes. :ref:https://docs.aws.amazon.com/general/latest/gr/rande.html.

Attribut	Description
Accept Self-signed Cert (Accepter le certificat autosigné)	Est automatiquement marqué comme vrai pour AWS. L'utilisateur ne peut pas le modifier.
Intervalle complet entre les instantanés	Intervalle de l'instantané complet en secondes. Le gestionnaire d'inventaire de l'orchestrateur effectuera une interrogation d'actualisation complète à partir de l'orchestrateur.
Intervalle différentiel entre les instantanés	Intervalle de l'instantané différentiel en secondes. Le gestionnaire d'inventaire de l'orchestrateur récupérera uniquement les mises à jour incrémentielles de l'orchestrateur.
Liste d'hôtes	Le type d'orchestrateur AWS ne nécessite pas de liste d'hôtes. Le point d'terminal pour AWS sera dérivé du champ *AWS Region* ci-dessus. Ce champ doit être laissé vide.
Mesures TSDB détaillées	Si cette option est activée, les mesures tsdb pour chaque orchestrateur individuel seront rapportées. Sinon, une agrégation de toutes les mesures de l'orchestrateur sera rapportée.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Tunneliser les connexions vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel de Connecteur sécurisé.

Flux de travaux

- Configurez un orchestrateur AWS avec les champs de configuration ci-dessus.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes suivantes à toutes les instances AWS.

Clé	Valeur
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	*<Nom de la grappe Kubernetes>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/cluster_id	*<UUID de la configuration de l'orchestrateur dans |produit|>*

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à l'instance.

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*<Numéro d'instance attribué par AWS>*
orchestrator_system/machine_name	*<PublicDNS(nom de domaine complet (FQDN)) donné à ce nœud par AWS>*
orchestrator_'<Clé d'étiquette AWS>'	*<Valeur de l'étiquette AWS>*

Dépannage

- Confusion entre la région AWS et la zone de disponibilité

  Ces deux valeurs sont interdépendantes et ne doivent pas être confondues. Par exemple, us-ouest-1 pourrait être la région et la zone de disponibilité peut être us-ouest-1a ou us-ouest-1b, etc. Lors de la configuration de l'orchestrateur, la *région* doit être utilisée. Reportez-vous à https://docs.aws.amazon.com/general/latest/gr/rande.html pour toutes les régions.

- Problème de connectivité et de renseignements d'authentification après la mise à jour de la configuration de l'orchestrateur

  Les clients doivent soumettre de nouveau la *clé secrète AWS* chaque fois que la configuration est mise à jour.

Kubernetes/OpenShift

Note Les fonctionnalités des orchestrateurs externes EKS et AKS font désormais partie des nouvelles fonctionnalités des connecteurs infonuagiques AWS et Azure, respectivement. Si vous avez effectué la mise à niveau vers cette version, vos orchestrateurs externes EKS et AKS existants sont maintenant en lecture seule; si vous devez apporter des modifications, créez un nouveau connecteur AWS ou Azure. Pour des renseignements complets, consultez les rubriques pertinentes sous connecteurs infonuagiques.

L'orchestrateur externe pour Kubernetes et OpenShift standard n'a pas été modifié.

Cisco Secure Workload prend en charge l'acquisition automatisée de l'inventaire en direct à partir d'une grappe Kubernetes. Lorsqu'une configuration d'orchestrateur externe est ajoutée pour une grappe Kubernetes/OpenShift, Cisco Secure Workload se connecte au serveur d'API de la grappe et suit l'état des nœuds, des pods et des services dans cette grappe. Pour chaque type d'objet, Cisco Secure Workload importe toutes les étiquettes Kubernetes et les étiquettes associées à l'objet. Toutes les valeurs sont importées en l'état.

En plus d'importer les étiquettes définies pour les objets Kubernetes/OpenShift, Cisco Secure Workload génère également des étiquettes qui facilitent l'utilisation de ces objets dans les filtres d'inventaire. Ces étiquettes supplémentaires sont particulièrement utiles pour définir les portées et les politiques.

Pour en savoir plus sur toutes ces étiquettes, consultez Étiquettes liées aux grappes Kubernetes.

Si l'application est activée sur les nœuds Kubernetes (les agents d'application sont installés et le profil de configuration active l'application sur ces agents), les politiques d'application seront installées à la fois sur les nœuds et à l'intérieur des espaces de noms des pods en utilisant les informations acquises sur les entités Kubernetes par le biais de cette intégration.

À propos de Kubernetes sur les plateformes infonuagiques

Pour les services Kubernetes gérés suivants qui s'exécutent sur des plateformes infonuagiques prises en charge, la fonctionnalité de cet orchestrateur est fournie à l'aide de connecteurs infonuagiques :

- Elastic Kubernetes Service (EKS) s'exécutant sur Amazon Web Services (AWS)
- Azure Kubernetes Service (AKS) s'exécutant sur Microsoft Azure
- Google Kubernetes Engine (GKE) s'exécutant sur Google Cloud Platform (GCP)

Pour plus de détails sur l'obtention de données à partir de grappes Kubernetes sur les plateformes infonuagiques, consultez les rubriques sous connecteurs infonuagiques.

Exigences et prérequis

- Pour les versions de Kubernetes et d'OpenShift prises en charge, consultez https://www.cisco.com/go/secure-workload/requirements/integrations
- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité.

Champs de configuration

Les champs de configuration suivants concernent la configuration de l'orchestrateur Kubernetes dans l'objet Orchestrateur.

Champ	Description
Nom	Nom de l'orchestrateur spécifié par l'utilisateur.
Description	Description de l'orchestrateur précisée par l'utilisateur.
Intervalle différentiel	Intervalle (en secondes) pour vérifier les modifications sur le point terminal Kubernetes
Intervalle complet entre les instantanés	Intervalle (en secondes) pour effectuer un instantané complet des données Kubernetes
Nom d'utilisateur	Nom d'utilisateur pour le point terminal de l'orchestration.
Mot de passe	Mot de passe du point terminal de l'orchestration.
Certificat	Votre certificat client servira à l'authentification.
Clé	Clé correspondant au certificat client.

Champ	Description
Jeton d'authentification	Jeton d'authentification opaque (jeton porteur).
Certificat de l'autorité de certification	Certificat de l'autorité de certification pour valider le point terminal de l'orchestration.
Accept Self-signed Cert (Accepter le certificat autosigné)	Case pour désactiver la vérification SSL stricte du certificat du serveur d'API Kubernetes
Mesures TSDB détaillées	Maintenir les mesures par Kubernetesorchestrator – si la valeur est faux, seules les mesures à l'échelle de la grappe Cisco Secure Workload sont conservées.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Connexions de tunnel vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel du connecteur sécurisé
Liste d'hôtes	Tableau de paires { « host_name », « port_number »,} (nom de l'hôte, numéro de port) qui précisent comment Cisco Secure Workload doit se connecter à l'orchestrateur
Type de gestionnaire K8	Type de gestionnaire pour la grappe Kubernetes (aucun pour les déploiements standard/OpenShift Kubernetes)
Nom de la grappe AWS	Nom de l'orchestrateur comme spécifié au moment de la création de la grappe (EKS préexistant)
ID d'accès AWS	CLÉ D'ACCÈS associée au compte pour lequel la configuration de l'orchestrateur est créée (EKS préexistant)
Clé d'accès secrète AWS	La CLÉ SECRÈTE associée au compte pour lequel la configuration de l'orchestrateur est créée. Saisissez à nouveau la clé secrète chaque fois que la configuration est modifiée. (EKS pré-existant)
Région AWS	La région dans laquelle la charge de travail a été déployée. Si une charge de travail est répartie sur plusieurs régions, une configuration distincte est requise pour chaque région. Consultez le lien ci-dessous pour connaître les valeurs de *région* correctes. :ref: https://docs.aws.amazon.com/general/latest/gr/rande.html. (EKS pré-existant)
ARN Assume Role AWS	Numéro de ressource Amazon des rôles à assumer lors de la connexion à l'outil d'orchestration : https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html (EKS préexistant) .

Champ	Description
ID du détenteur Azure	Identifiant du détenteur associé à l'abonnement Azure. (AKS pré-existant uniquement)
ID du client Azure	Identifiant global unique associé à l'application qui doit s'authentifier auprès d'Azure AD. (AKS pré-existant uniquement)
Code secret du client Azure	Mot de passe associé au principal service pour l'application qui doit s'authentifier auprès d'Azure AD. (AKS pré-existant uniquement)

Règles d'or de l'orchestrateur

Les attributs d'objet des règles d'or sont décrits ci-dessous. Ces règles d'or permettent de préciser les règles nécessaires à la grappe Kubernetes pour rester fonctionnelle une fois que la mise en application est activée sur les nœuds de la grappe Kubernetes.

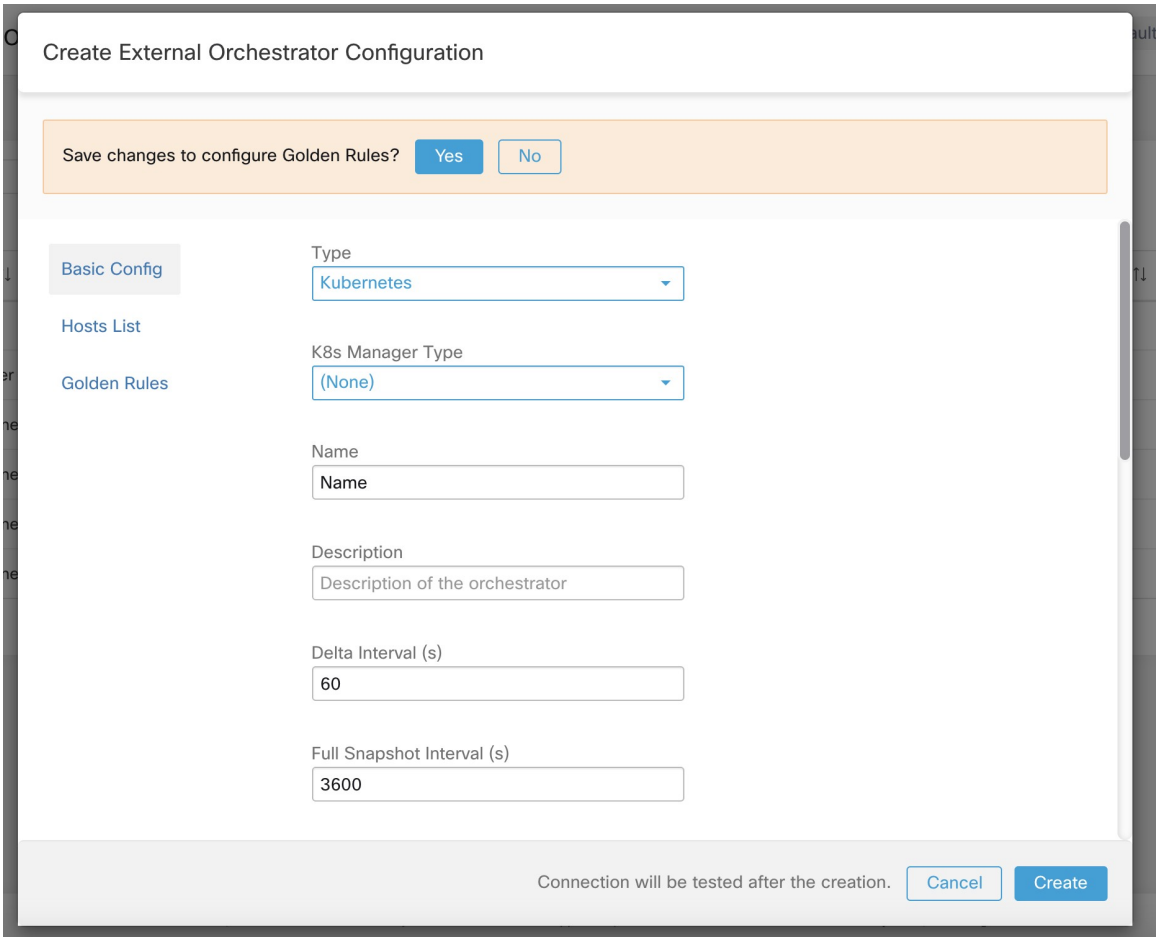
Attribut	Description
Port Kubelet	Port d'API local au nœud de Kubelet
Services	Tableau d'objets des services Kubernetes

Le port Kubelet est nécessaire pour créer des politiques autorisant le trafic des daemons de gestion Kubernetes vers les kubelets, par exemple pour les journaux en direct, les exécutions de pods en mode interactif, etc. La connectivité vitale entre les différents services et daemons Kubernetes est spécifiée sous la forme d'une série de services - chaque entrée du tableau de services a la structure suivante :

- Description : une chaîne qui décrit le service.
- Addresses : une liste d'adresses de points terminaux de service du format <IP>:<port> /<protocol> .
- Consommé par : une liste des consommateurs des points terminaux (les valeurs autorisées sont les pods ou les nœuds)

Note Si **Kubernetes** est choisi comme type, la configuration des règles d'or sera autorisée.

Figure 53: Créer une configuration de règles d'or pour le type Kubernetes



Flux de travaux

- Configurez le tunnel du connecteur sécurisé, si nécessaire, pour la connectivité de la grappe Cisco Secure Workload à un serveur ou des serveurs d'API Kubernetes.
- Configurez un orchestrateur Kubernetes rempli avec les champs de configuration ci-dessus.
- Configurez les règles d'or pour l'orchestrateur Kubernetes.

Considérations relatives aux ressources pour le contrôle d'accès en fonction des rôles (Role-Based Access Control ou RBAC) de Kubernetes

Le client Kubernetes tente de RECEVOIR/RÉPERTORIER/SURVEILLER les ressources suivantes. Il est fortement recommandé de NE PAS configurer la clé ou le certificat d'administrateur ou un compte de service administrateur.

Les informations d'authentification Kubernetes fournies doivent avoir un ensemble minimal de privilèges sur les ressources suivantes :

Ressources	Verbes Kubernetes
points terminaux	[obtenir la liste de surveillance]
espaces de noms	[obtenir la liste de surveillance]
nœuds	[obtenir la liste de surveillance]
pods	[obtenir la liste de surveillance]
services	[obtenir la liste de surveillance]
entrées	[obtenir la liste de surveillance]
contrôleurs de duplication	[obtenir la liste de surveillance]
jeux de répliques	[obtenir la liste de surveillance]
déploiements	[obtenir la liste de surveillance]
daemonsets	[obtenir la liste de surveillance]
statefulsets	[obtenir la liste de surveillance]
tâches	[obtenir la liste de surveillance]
cronjobs	[obtenir la liste de surveillance]

En substance, vous pouvez créer un compte de service spécial sur votre serveur Kubernetes avec ces privilèges minimaux. Vous trouverez ci-dessous un exemple de séquence de commandes kubectl qui facilitera la création de ce compte de service. Notez l'utilisation de clusterrole (non de rôle) et clusterrolebindings (non de rolebindings) - ce sont des rôles à l'échelle de la grappe et non d'un espace de nom. L'utilisation d'une liaison de rôle ou de rôle ne fonctionnera pas, car Cisco Secure Workload tente de récupérer les données de tous les espaces de noms.

```
$ kubectl create serviceaccount csw.read.only
```

Créez le rôle de grappe (clusterrole).

Un exemple de fichier clusterrole.yaml avec des privilèges minimaux est fourni ci-dessous.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: csw.read.only
rules:
  - apiGroups:
    - ""
    resources:
      - nodes
      - services
      - endpoints
      - namespaces
      - pods
      - replicationcontrollers
      - ingresses
    verbs:
      - get
```

```
      - list
      - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
    resources:
      - ingresses
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - apps
    resources:
      - replicasets
      - deployments
      - statefulsets
      - daemonsets
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - batch
    resources:
      - jobs
      - cronjobs
    verbs:
      - get
      - list
      - watch

$ kubectl create -f clusterrole.yaml
```

Note Les groupes d'API pour ces différentes ressources sont susceptibles de changer selon les versions de Kubernetes. L'exemple ci-dessus devrait fonctionner pour les versions 1.20 à 1.24 de Kubernetes et pourrait nécessiter quelques ajustements pour d'autres versions.

Créer la liaison de rôles de grappe

```
$ kubectl create clusterrolebinding csw.read.only --clusterrole=csw.read.
‹→only --serviceaccount=default:csw.read.only
```

Pour récupérer le code secret authtoken du compte de service (utilisé dans le champ Auth Token dans l'interface graphique) et le décoder en base64, vous pouvez récupérer le nom du code secret en listant le compte de service avec la sortie yaml.

```
$ kubectl get serviceaccount -o yaml csw.read.only
apiVersion: v1
kind: ServiceAccount
metadata:
  creationTimestamp: 2020-xx-xxT19:59:57Z
  name: csw.read.only
  namespace: default
  resourceVersion: "991"
  selfLink: /api/v1/namespaces/default/serviceaccounts/e2e.minimal
  uid: ce23da52-a11d-11ea-a990-525400d58002
secrets:
- name: csw.read.only-token-vmvmz
```

Lister le code secret en mode de sortie yaml produira le jeton mais au format Base64 (ce qui est la procédure standard de Kubernetes pour les données secrètes). Cisco Secure Workload n'accepte pas le jeton dans ce format, vous devez le décoder à partir de Base64.

```
$ kubectl get secret -o yaml csw.read.only-token-vmvmz
apiVersion: v1
data:
  ca.crt: ...
  namespace: ZGVmYXVsdA==
  token: ZXlKaGJHY2lPaUpTVX....HRfZ2JwMVZR
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: csw.read.only
    kubernetes.io/service-account.uid: ce23da52-a11d-11ea-a990-525400d58002
  creationTimestamp: 2020-05-28T19:59:57Z
  name: csw.read.only-token-vmvmz
  namespace: default
  resourceVersion: "990"
  selfLink: /api/v1/namespaces/default/secrets/csw.read.only-token-vmvmz
  uid: ce24f40c-a11d-11ea-a990-525400d58002
type: kubernetes.io/service-account-token
```

Pour répertorier le code secret et afficher uniquement le champ `.data.token` et décoder le codage en base 64 en une seule commande, la commande suivante qui utilise l'option `--template` est utile.

```
  $ kubectl get secret csw.read.only-token-vmvmz --template "{{ .data.token }}" | base64
-d
```

Cet authtoken peut être utilisé pour configurer un orchestrateur Kubernetes dans l'interface utilisateur Cisco Secure Workload au lieu de nom d'utilisateur/mot de passe ou de clé/certificat.

Consultez la section Considérations relatives à RBAC spécifiques à EKS.

Étiquettes générées par l'orchestrateur

Consultez la section Étiquettes liées aux grappes Kubernetes.

Dépannage

- Analyse ou incompatibilité des informations d'authentification de la clé ou du certificat client

  Celles-ci doivent être fournies au format PEM et correspondre à l'entrée correcte du fichier kubectl.conf. Nous avons rencontré des clients qui collaient des certificats d'autorité de certification dans les champs de certificats des clients, ainsi que des clés et des certificats qui ne correspondaient pas les uns aux autres.

- Identifiants Gcloud au lieu des identifiants GKE

  Les clients qui utilisent GKE sous la ligne de commande gcloud fournissent par erreur les informations d'authentification gcloud alors que les informations d'authentification de grappe GKE sont nécessaires.

- Version de la grappe Kubernetes non prise en charge

  L'utilisation d'une version incompatible de Kubernetes peut entraîner des défaillances. Vérifiez que la version de Kubernetes figure dans la liste des versions prises en charge.

- Les informations d'authentification ont des privilèges insuffisants

Vérifiez que le jeton d'authentification ou la clé d'utilisateur client, ou le certificat utilisé dispose de tous les privilèges répertoriés dans le tableau ci-dessus.

- L'inventaire Kubernetes n'en finit pas de basculer

  Le champ hosts_list spécifie un groupe de serveurs d'API pour la même grappe Kubernetes – vous ne pouvez pas l'utiliser pour configurer plusieurs grappes Kubernetes. Cisco Secure Workload vérifiera la réactivité et sélectionnera aléatoirement l'un de ces points terminaux pour s'y connecter et récupérer les informations de l'inventaire Kubernetes. Aucun équilibrage de charge n'est effectué ici, et il n'y a aucune garantie de répartition uniforme de la charge sur ces points terminaux. S'il s'agit de grappes différentes, l'inventaire de Kubernetes continuera à basculer entre elles, selon le serveur d'API de la grappe auquel nous nous connectons.

- Plusieurs méthodes d'autorisation

  Plusieurs méthodes d'autorisation peuvent être saisies lors de la configuration (nom d'utilisateur ou mot de passe, authtoken, clé ou certificat client) et seront utilisées dans la connexion client établie avec le serveur d'API. Les règles standard de Kubernetes concernant les méthodes d'autorisation simultanée valides s'appliquent ici.

- La validation du certificat SSL échoue

  Si le point de terminaison de l'API Kubernetes se trouve derrière un NAT ou un équilibreur de charge, le numéro de répertoire (NR) dans le certificat SSL généré sur les nœuds du plan de contrôle Kubernetes peut ne pas correspondre à l'adresse IP configurée dans Cisco Secure Workload. Cela entraînera un échec de validation SSL même si le certificat de l'autorité de certification est fourni et valide. Le bouton Insecure (Non sécurisé) contourne la validation stricte des certificats SSL du serveur et aidera à contourner ce problème, mais peut entraîner des problèmes de MITM. Le correctif correct consiste à modifier le certificat de l'autorité de certification pour fournir des entrées SAN (Subject Alternative Name) pour toutes les entrées DNS ou IP qui peuvent être utilisées pour se connecter à la grappe Kubernetes.

VMware vCenter

L'intégration de vCenter permet à l'utilisateur de récupérer les attributs sans système d'exploitation et de machine virtuelle du vCenter configuré.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « vCenter », Cisco Secure Workload récupère les attributs de machines sans système d'exploitation et de VM pour toutes les machines sans système d'exploitation et les machines virtuelles contrôlées par cette instance de vCenter. Cisco Secure Workload importera les attributs suivants d'une machine virtuelle ou d'une machine sans système d'exploitation : a) le nom d'hôte b) les adresses IP c) l'UUID BIOS d) les catégories/étiquettes.

Un nouvel inventaire sera créé dans Cisco Secure Workload avec les attributs de machines sans système d'exploitation et des machines virtuelles ci-dessus, si l'inventaire n'est pas présent dans l'appareil. Si l'inventaire est déjà présent dans l'appareil (créé par le capteur de visibilité Cisco Secure Workload fonctionnant sur l'ordinateur sans système d'exploitation/la machine virtuelle), l'inventaire existant sera étiqueté avec la liste des catégories/étiquettes d'ordinateurs sans système d'exploitation/de VM récupérés.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité.
- La version de vCenter prise en charge est la 6.5+

Champs de configuration

En plus des champs de configuration courants, décrits dans la section*Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

- **La liste des hôtes** est un tableau de paires de nom d'hôte/IP et de ports pointant vers le serveur vCenter à partir duquel les attributs de machines sans système d'exploitation/de machines virtuelles seront extraits.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur vCenter est accessible sur cette adresse IP/ce port à partir de la grappe Cisco Secure Workload.
- Pour TaaS ou dans les cas où le serveur vCenter n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes suivantes à toutes les machines virtuelles apprises du serveur vCenter.

Clé	Valeur
orchestrator_system/orch_type	vCenter
orchestrator_system/cluster_name	*<Nom donné à la configuration de cette grappe>*
orchestrator_system/cluster_id	*<L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload>*

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à l'instance.

Table 16: Les étiquettes suivantes sont propres à l'instance.

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*UUID BIOS de machine sans système d'exploitation/VM*
orchestrator_system/machine_name	*Nom d'hôte de la machine sans système d'exploitation/de la machine virtuelle*
orchestrator_'<Category Name>'	*<Tag Value>*

Mises en garde

- Lorsqu'une configuration d'orchestrateur externe est ajoutée à vCenter, le logiciel Cisco Secure Workload se connecte au serveur vCenter spécifié dans la liste d'hôtes. Une fois la connexion au serveur réussie, le logiciel Cisco Secure Workload importera les noms d'hôte, les adresses IP et les catégories ou étiquettes pour toutes les machines sans système d'exploitation et les machines virtuelles présentes sur le serveur vCenter. Pour importer les noms d'hôte et les adresses IP de la machine sans système d'exploitation et des machines virtuelles, les outils de VM doivent être installés sur l'ensemble de la machine sans système d'exploitation et les machines virtuelles. Si les outils VM ne sont pas installés pour une machine virtuelle ou sans système d'exploitation, le logiciel Cisco Secure Workload n'affichera pas les catégories ou les étiquettes pour cette machine virtuelle ou sans système d'exploitation en particulier.
- Le logiciel Cisco Secure Workload n'importe pas les attributs personnalisés du logiciel sans système d'exploitation ou de la machine virtuelle.
- Il est recommandé de fixer la durée de minuterie de l'intervalle **Delta** à plus de 10 minutes afin de réduire la charge sur le serveur vCenter. Toute modification de l'inventaire ou des étiquettes sur le serveur vCenter aura un délai de propagation d'au moins 10 min, une fois la minuterie mentionnée ci-dessus modifiée.

Dépannage

- Problèmes de connexion

  Si le dispositif Cisco Secure Workload ne peut pas se connecter ou atteindre le serveur vCenter, l'onglet **Connection Status** (État de la connexion) de l'orchestrateur externe affichera l'état de l'échec ainsi que l'erreur appropriée, le cas échéant.

- Contrôle de l'intégrité du logiciel Cisco Secure Workload.

  Consultez la page **MAINTENANCE/Service Status** (MAINTENANCE/état de service) pour voir si un service est en panne. Vérifiez si **OrchestratorInventoryManager** est opérationnel et fonctionne.

DNS

L'intégration du DNS permet à Cisco Secure Workload d'annoter un inventaire connu avec des renseignements DNS tels que les noms d'hôte des enregistrements CNAME et A/AAAA.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « dns », l'appareil Cisco Secure Workload tente de se connecter au(x) serveur(s) DNS et effectue un téléchargement de transfert de zone des enregistrements DNS. Ces enregistrements (uniquement les enregistrements A/AAAA et CNAME) seront analysés et utilisés pour enrichir l'inventaire dans les pipelines Cisco Secure Workload (comme appartenant au détenteur sous lequel l'orchestrateur est configuré) avec une seule étiquette à valeurs multiples appelée « orchestrator_system/dns_name », dont la valeur correspond aux entrées DNS qui pointent (directement ou indirectement) vers cette adresse IP.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité

- Serveurs DNS pris en charge : BIND9, serveurs prenant en charge AXFR (RFC 5936), Microsoft Windows Server 2016

Champs de configuration

- **Les zones DNS** sont un tableau de chaînes, dont chacune représente une zone DNS à transférer à partir du serveur DNS. Toutes les zones DNS doivent être précédées d'un point (« . »).
- **La liste d'hôtes** est un tableau de paires de nom d'hôte/adresse IP et de paires de port pointant vers le ou les serveurs DNS à partir duquel récupérer les enregistrements DNS. Plusieurs serveurs DNS peuvent être configurés ici à des fins de haute disponibilité uniquement. Le comportement de haute disponibilité sur plusieurs serveurs DNS spécifiés dans hosts_list est celui de « premier serveur intègre » et favorisera les entrées les plus anciennes de hosts_list. Les zones ne peuvent pas être fractionnées sur les serveurs DNS.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur DNS est accessible sur cette adresse IP/ce port à partir de la grappe Cisco Secure Workload.
- Pour le TaaS ou dans les cas où le serveur DNS n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Configurez correctement les ACL/la configuration des transferts de zone DNS sur le serveur DNS. Reportez-vous à la documentation du logiciel de serveur DNS correspondant pour obtenir de plus amples renseignements.

Étiquettes générées

orchestrator_system/dns_name -> un champ à valeurs multiples dont les valeurs sont tous les noms d'hôte CNAME et A/AAAA pointant vers cette adresse IP.

Mises en garde

- Le flux de l'orchestrateur DNS est un *flux de métadonnées* : les adresses IP apprises lors d'un transfert de zone DNS ne créeront pas d'éléments d'inventaire dans Cisco Secure Workload. Au contraire, les étiquettes d'une adresse IP existante seront mises à jour avec les nouvelles métadonnées DNS. Les données DNS des adresses IP inconnues sont rejetées en mode silencieux. Afin d'annoter les métadonnées DNS des IP qui n'ont pas été apprises par un capteur ou via d'autres intégrations d'orchestrateur, les adresses IP doivent être téléversées via le mécanisme de téléversement en bloc de la CMDB afin de créer des entrées d'inventaire pour ces adresses. Les sous-réseaux appris des téléchargements CMDB ne créent pas d'entrées d'inventaire.
- Seuls les enregistrements CNAME et A/AAAA du serveur DNS sont traités. Les enregistrements CNAME seront transformés en enregistrements IPv4/IPv6 finaux via les enregistrements A/AAAA vers lesquels ils pointent. Un seul niveau de déférencement est pris en charge (c.-à-d. les chaînes CNAME -> CNAME -> A/AAAA ou plus ne sont pas déférencées) tant que CNAME pointe vers un enregistrement A/AAAA du même orchestrateur. Le déférencement CNAME sur différents orchestrateurs DNS n'est pas pris en charge.

Dépannage

- Problèmes de connexion

  Cisco Secure Workload tentera de se connecter au nom d'adresse IP/nom d'hôte et au numéro de port fournis en utilisant une connexion TCP provenant de l'un des serveurs d'appareils Cisco Secure Workload, du nuage dans le cas de TaaS, ou de la machine virtuelle hébergeant le service de tunnel VPN de connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic.

- Problèmes de privilège DNS AXFR

  De plus, la plupart des serveurs DNS (BIND9 ou Windows DNS ou Infoblox) nécessitent une configuration supplémentaire lorsque les adresses IP des clients tentent des transferts de zone DNS (requêtes AXFR selon les codes d'opération du protocole DNS), car ceux-ci sont plus exigeants en ressources et privilégiés que de simples requêtes DNS pour résoudre des enregistrements DNS individuels. Ces erreurs s'affichent généralement comme un refus AXFR, avec le code de raison 5 (REFUSÉ).

  Ainsi, tout test manuel visant à établir que le serveur DNS est configuré correctement ne doit pas dépendre de recherches réussies de nom d'hôte, mais doit plutôt tester spécifiquement les requêtes AXFR (à l'aide d'un outil comme dig).

  Tout échec lors d'un transfert de zone AXFR à partir du serveur DNS sera signalé dans le champ « authentication_failure_error » par l'appareil Cisco Secure Workload.

  En outre, notez que Cisco Secure Workload tentera des transferts de zone à partir de toutes les zones DNS configurées et que toutes doivent réussir pour que les données DNS soient insérées dans la base de données d'étiquettes Cisco Secure Workload.

- Les champs de nom d'hôte de l'inventaire ne sont pas remplis par DNS. Le « nom d'hôte » est toujours appris à partir du capteur Cisco Secure Workload. Si l'inventaire a été téléversé par le téléchargement dans la CMDB et non à partir du capteur, il manque peut-être le nom d'hôte. Toutes les données du flux de travail de l'orchestrateur DNS ne s'affichent que sous l'étiquette « orchestrator_system/dns_name » et ne rempliront jamais le champ du nom d'hôte.

Comportement de l'interrogation complète/additionnelle pour les orchestrateurs DNS

L'intervalle par défaut des instantanés complets est de 24 heures

L'intervalle par défaut des instantanés différentiels est de 60 minutes

Il s'agit également des valeurs minimales autorisées pour ces minuteurs.

Les enregistrements DNS ne changent que rarement. Ainsi, pour un comportement de récupération optimale, à chaque intervalle d'instantané différentiel, Cisco Secure Workload vérifie si les numéros de série de l'une des zones DNS ont modifié par rapport à l'intervalle précédent. Si aucune zone n'a changé, aucune action n'est nécessaire.

Si des zones ont été modifiées, nous effectuerons un transfert de zone à partir de toutes les zones DNS configurées (pas seulement de la zone qui a été modifiée).

À chaque intervalle d'instantané complet, les transferts de zone sont téléchargés à partir de toutes les zones et injectés par Cisco Secure Workload dans la base de données des étiquettes, que les numéros de série des zones aient changé ou non.

Fonctionnalités non prises en charge

Warning

- Les alias et les recherches DNAME ne sont pas pris en charge.
- Les transferts de zone incrémentiels (IXFR) ne sont pas pris en charge.

Infoblox

L'intégration Infoblox permet à Cisco Secure Workload d'importer des sous-réseaux Infoblox, des hôtes (*Record:host*) et des enregistrements A/AAAA dans la base de données d'inventaire de Cisco Secure Workload. Les noms et les valeurs des attributs extensibles sont importés tels quels et peuvent être utilisés comme étiquettes Cisco Secure Workload pour définir la portée et les politiques d'application.

Note Seuls les objets Infoblox avec des attributs extensibles sont pris en compte, c.-à-d. ceux auxquels aucun attribut extensible n'est attaché seront exclus de l'importation.

L'image ci-dessous montre un exemple d'étiquettes générées pour un objet hôte importé d'Infoblox avec l'attribut extensible *Department* :

Figure 54: Exemples d'étiquettes Infoblox

```
1. orchestrator_Department = AES789
2. orchestrator_system/cluster_id = [redacted]
3. orchestrator_system/cluster_name = scale13-ib
4. orchestrator_system/machine_id =
   record:host/[redacted]:client8/%20
5. orchestrator_system/machine_name = client8
6. orchestrator_system/orch_type = infoblox
```

Prérequis

- Point terminal d'API REST Infoblox prenant en charge WAPI version 2.6, 2.6.1, 2.7 et 2.7.1 (recommandé)

Champs de configuration

En plus des champs de configuration courants, décrits dans la section*Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Liste d'hôtes	Oui	La liste des hôtes indique une grille Infoblox, c'est-à-dire que plusieurs membres de la grille avec accès à l'API REST peuvent être ajoutés, et l'orchestrateur externe passera à la grille suivante dans la liste en cas d'erreurs de connexion. Si vous souhaitez importer des étiquettes d'une autre grille Infoblox, créez un nouvel orchestrateur externe pour celle-ci.

Note Pour les orchestrateurs externes Infoblox, les adresses IPv4 et IPv6 (mode pile double) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST Infoblox est accessible à partir de la grappe Cisco Secure Workload.
- Dans l cas du TaaS ou lorsque le serveur Infoblox n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Créez un orchestrateur externe de type *Infoblox*. Selon le volume des données Infoblox, c'est-à-dire le nombre de sous-réseaux, d'hôtes et d'enregistrements A/AAAA, il peut s'écouler jusqu'à une heure avant que le premier instantané complet soit disponible dans Cisco Secure Workload.
- Lors de la création de la configuration Infoblox, l'utilisateur a la possibilité de désélectionner n'importe quel type d'enregistrement (sous-réseau, hôte, enregistrements A/AAAA).

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes à tous les objets extraits d'Infoblox.

Clé	Valeur
orchestrator_system/orch_type	infoblox
orchestrator_system/cluster_id	UUID de l'orchestrateur externe dans Cisco Secure Workload
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/machine_id	<Référence/identifiant de l'objet Infoblox>
orchestrator_system/machine_name	<nom de l'hôte Infoblox (DNS)>

Étiquettes générées

Tous les attributs extensibles Infoblox seront importés en tant qu'étiquettes Cisco Secure Workload avec le préfixe *orchestrator_*. Par exemple, un hôte avec un attribut extensible appelé *Department* (service) peut être appelé dans la recherche d'inventaire Cisco Secure Workload en tant que *service_orchestrateur*.

Clé	Valeur
orchestrator_<extensible attribute>	<valeur(s) de l'attribut extensible telle(s) qu'extraite(s) d'Infoblox>

Mises en garde

- Le nombre maximal de sous-réseaux pouvant être importés à partir d'Infoblox est de 50 000.
- Le nombre maximal d'hôtes et d'enregistrements A/AAAA qui peuvent être importés à partir d'Infoblox est de 400 000 au total.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de TaaS , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez des privilèges pour envoyer des demandes d'API REST à l'appareil Infoblox.
- Tous les objets attendus ne sont pas importés. Cisco Secure Workload importe uniquement des sous-réseaux, des hôtes et des enregistrements A/AAAA auxquels des attributs extensibles sont attachés. Notez qu'il y a une limite au nombre d'objets qui peuvent être importés d'Infoblox, consultez *Mises en garde*.
- Impossible de trouver des sous-réseaux dans l'inventaire Il n'est pas possible d'utiliser la recherche dans l'inventaire pour trouver des sous-réseaux Infoblox car l'inventaire Cisco Secure Workload par conception ne comporte que des adresses IP, c'est-à-dire des hôtes et des enregistrements A/AAA.
- Impossible de trouver un hôte ou un enregistrement A/AAAA, Cisco Secure Workload importe tous les attributs extensibles tels qu'ils ont été récupérés d'Infoblox. N'oubliez pas d'ajouter le préfixe *orchestrator_* au nom de l'attribut extensible, dans p. ex. la recherche d'inventaire. Notez que les attributs extensibles des sous-réseaux, s'ils ne sont pas marqués comme hérités dans Infoblox, ne font pas partie des hôtes et ne peuvent donc pas être recherchés dans Cisco Secure Workload.

F5 BIG-IP

L'intégration F5 BIG-IP permet à Cisco Secure Workload d'importer les *serveurs virtuels* à partir d'un dispositif d'équilibreur de charge F5 BIG-IP et d'en dériver des inventaires de services. Un inventaire de service correspond à un serveur virtuel F5 BIG-IP, dont le service se caractérise par la *VIP* (adresse IP virtuelle), le protocole et le port. Une fois importé dans Cisco Secure Workload, cet inventaire de service aura des

étiquettes telles que *service_name*, qui peuvent être utilisées dans la recherche d'inventaire ainsi que pour créer des portées et des politiques Cisco Secure Workload.

Un des gros avantages de cette fonctionnalité est l'application des politiques, car l' *orchestrateur externe pour F5 BIG-IP* traduit les politiques Cisco Secure Workload en règles de sécurité attribuées au serveur virtuel et les déploie sur l'équilibreur de charge F5 BIG-IP au moyen de son API REST.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Point de terminaison d'API REST F5 BIG-IP, version 12.1.1

Champs de configuration

En plus des champs de configuration courants, décrits dans la section*Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champ	Obligatoire	Description
Liste d'hôtes	Oui	Ceci spécifie le point de terminaison de l'API REST pour l'équilibreur de charge F5 BIG-IP. Si la haute disponibilité est configurée pour F5 BIG-IP, saisissez le nœud membre de secours de sorte qu'en cas de basculement, l'orchestrateur externe bascule sur le nœud actuel. Si vous souhaitez importer des étiquettes d'un autre équilibreur de charge F5 BIG-IP, vous devez créer un nouvel orchestrateur externe.
Activer l'application	Non	La valeur par défaut est faux (non cochée). Si cette option est cochée, cette option permet à Cisco Secure Workload *l'application des politiques* afin de déployer les règles de politique de sécurité sur l'équilibreur de charge F5 BIG-IP correspondant. Notez que les renseignements d'authentification fournis doivent avoir un accès en écriture sur l'API REST F5 BIG-IP.

Champ	Obligatoire	Description
Domaine de routage	Non	La valeur par défaut est 0 (zéro). Le domaine de routage spécifie quels serveurs virtuels doivent être pris en compte par l'orchestrateur externe. Le nombre est déterminé par la liste des partitions affectées à un domaine de routage donné, et seuls les serveurs virtuels définis dans ces partitions seront importés dans Cisco Secure Workload.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST F5 BIG-IP est accessible à partir de Cisco Secure Workload.
- Pour le TaaS ou dans les cas où l'appareil F5 BIG-IP n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour assurer la connectivité.
- Créez un orchestrateur externe de type *F5 BIG-IP*.
- Selon la valeur de l' *intervalle*, le premier instantané complet des serveurs virtuels F5 BIG-IP peut prendre jusqu'à 60 secondes (intervalle par défaut). Par la suite, les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes pour un orchestrateur externe pour *F5 BIG-IP* :

Clé	Valeur
orchestrator_system/orch_type	F5
orchestrator_system/cluster_id	<UUID de l'orchestrateur externe>
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/workload_type	service
orchestrator_system/namespace	<Partition à laquelle appartient le serveur virtuel>
orchestrator_system/service_name	<Nom du serveur virtuel F5 BIG-IP>

Étiquettes générées

Pour chaque serveur virtuel, l'orchestrateur externe génère les étiquettes suivantes :

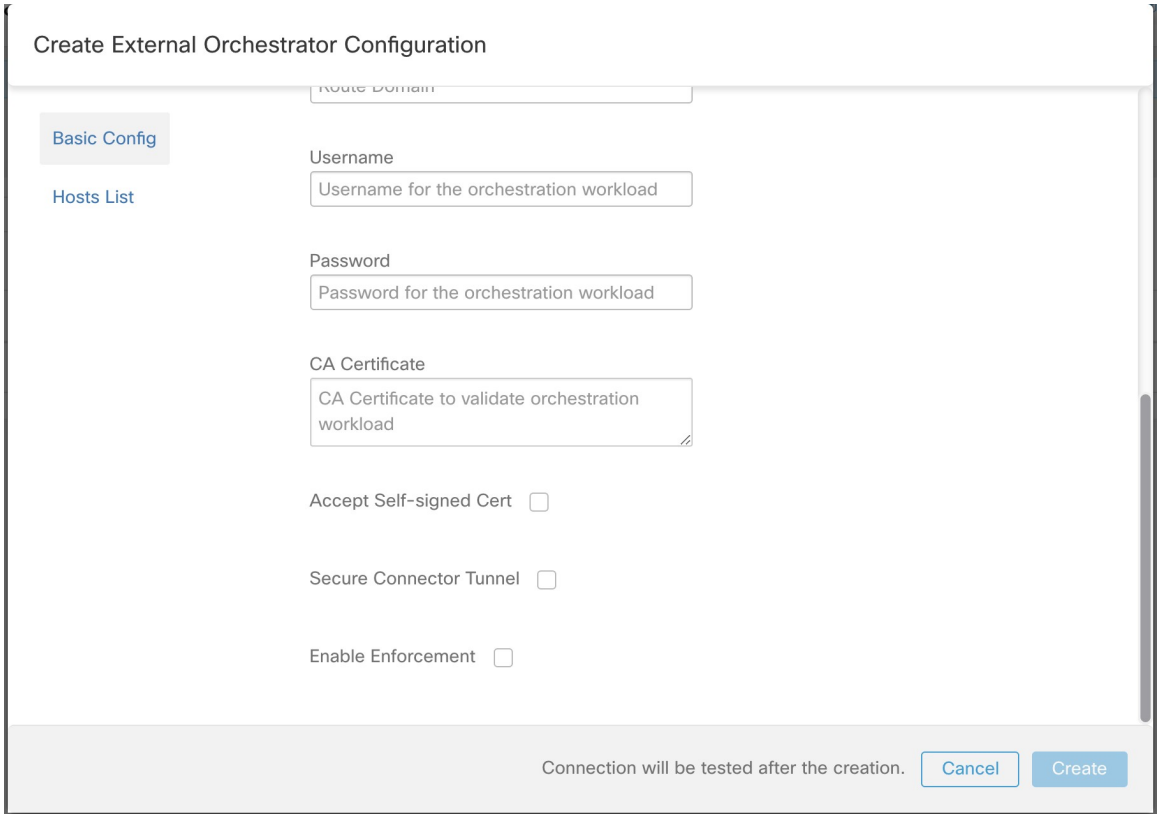
Clé	Valeur
orchestrator_annotation/snat_address	<Adresse SNAT des serveurs virtuels>

Application de la politique pour F5 BIG-IP

Cette fonctionnalité permet à Cisco Secure Workload de traduire les politiques logiques par des groupes de fournisseurs qui correspondent aux serveurs virtuels étiquetés *F5 BIG-IP* en règles de sécurité *F5 BIG-IP* et de les déployer sur le dispositif de l'équilibreur de charge à l'aide de son API REST. Comme mentionné ci-dessus, toute affectation de politique de sécurité existante au serveur virtuel *F5 BIG-IP* respectif sera remplacée par une nouvelle affectation pointant vers la politique de sécurité générée Cisco Secure Workload. Les politiques de sécurité existantes ne seront pas modifiées ni supprimées de la liste des politiques *F5 BIG-IP*.

Par défaut, l'application n'est pas activée dans la configuration de l'orchestrateur externe :

Figure 55: Option de configuration « Enable Enforcement » (Activer l'application)



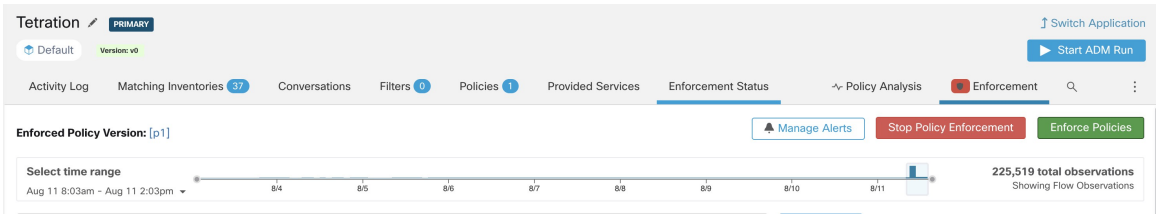
(Activer l'application)

Cette option peut être modifiée à tout moment au besoin.

L'activation de l'application ne déploie pas les politiques sur l'équilibreur de charge tant que l'application n'est pas activée dans un espace de travail comprenant au moins une politique applicable à l'équilibreur de charge, ou suite à des mises à jour d'inventaires.

Cependant, la désactivation de l'application pour l'orchestrateur entraînera la suppression immédiate de toutes les règles de politique de sécurité déployées de l'équilibreur de charge *F5 BIG-IP*.

Figure 56: Application des politiques de l'espace de travail



Note

- L'orchestrateur pour *F5 BIG-IP* détecte également tout écart des règles de politique de sécurité et le remplace par des politiques Cisco Secure Workload. Toute modification de politique envers les serveurs virtuels doit être effectuée qu'avec Cisco Secure Workload.
- Lorsque l'application de la politique est arrêtée ou que l'orchestrateur externe est supprimé, la politique de sécurité des serveurs virtuels deviendra vide, car toutes les politiques Cisco Secure Workload seront supprimées de l'équilibreur de charge *F5 BIG-IP*.

L'état d'application de la politique OpenAPI pour l'orchestrateur externe peut être utilisé pour récupérer l'état de l'application de la politique Cisco Secure Workload sur le dispositif de l'équilibreur de charge associé à l'orchestrateur externe. Cela permet de vérifier si le déploiement des règles de politique de sécurité sur l'appareil *F5 BIG-IP* a réussi ou échoué.

Application des politiques au contrôleur d'entrée F5

Cisco Secure Workload applique les politiques à la fois au niveau de l'équilibreur de charge *F5 BIG-IP* et au niveau des pods du backend lorsque les pods sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

Voici les étapes à suivre pour appliquer la politique à l'aide du contrôleur d'entrée F5.

Procedure

Étape 1 Créez un orchestrateur externe pour l'équilibreur de charge *F5 BIG-IP* , comme décrit précédemment.

Étape 2 Créez un orchestrateur externe pour Kubernetes/OpenShift comme décrit ici.

```
→  ~
→  ~ k8s get ingress
NAME           HOSTS   ADDRESS          PORTS   AGE
test-ingress   *       192.168.60.100   80      7s
→  ~
```

Étape 3 Créez un objet d'entrée dans la grappe Kubernetes. Un instantané du fichier yaml utilisé pour créer l'objet d'entrée est fourni dans l'image suivante.

```
→  ~
→  ~ k8s get ingress test-ingress -o yaml
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  annotations:
    virtual-server.f5.com/ip: 192.168.60.100
    virtual-server.f5.com/partition: k8scluster
  creationTimestamp: "2019-07-26T18:34:39Z"
  generation: 1
  name: test-ingress
  namespace: default
  resourceVersion: "8310"
  selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/test-ingress
  uid: 06f8a705-afd4-11e9-97fb-525400d58002
spec:
  backend:
    serviceName: nginx
    servicePort: 80
status:
  loadBalancer:
    ingress:
    - ip: 192.168.60.100
→  ~
```

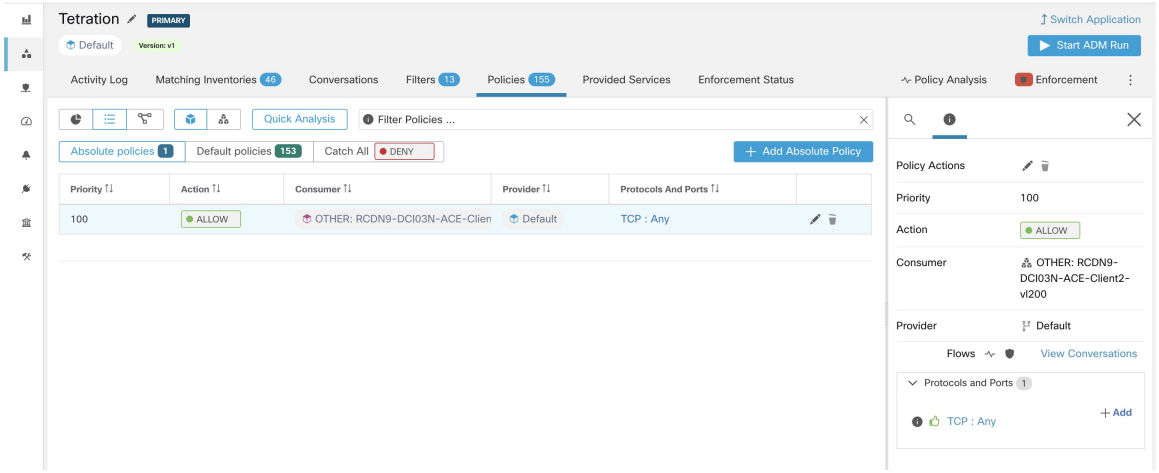
Étape 4 Déployez un pod de contrôleur d'entrée F5 dans la grappe Kubernetes.

```
→  ~ k8s get deploy -n kube-system
NAME                    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
coredns                 2         2         2            2           31m
k8s-bigip-ctlr-cluster  1         1         1            1           5m20s
→  ~
```

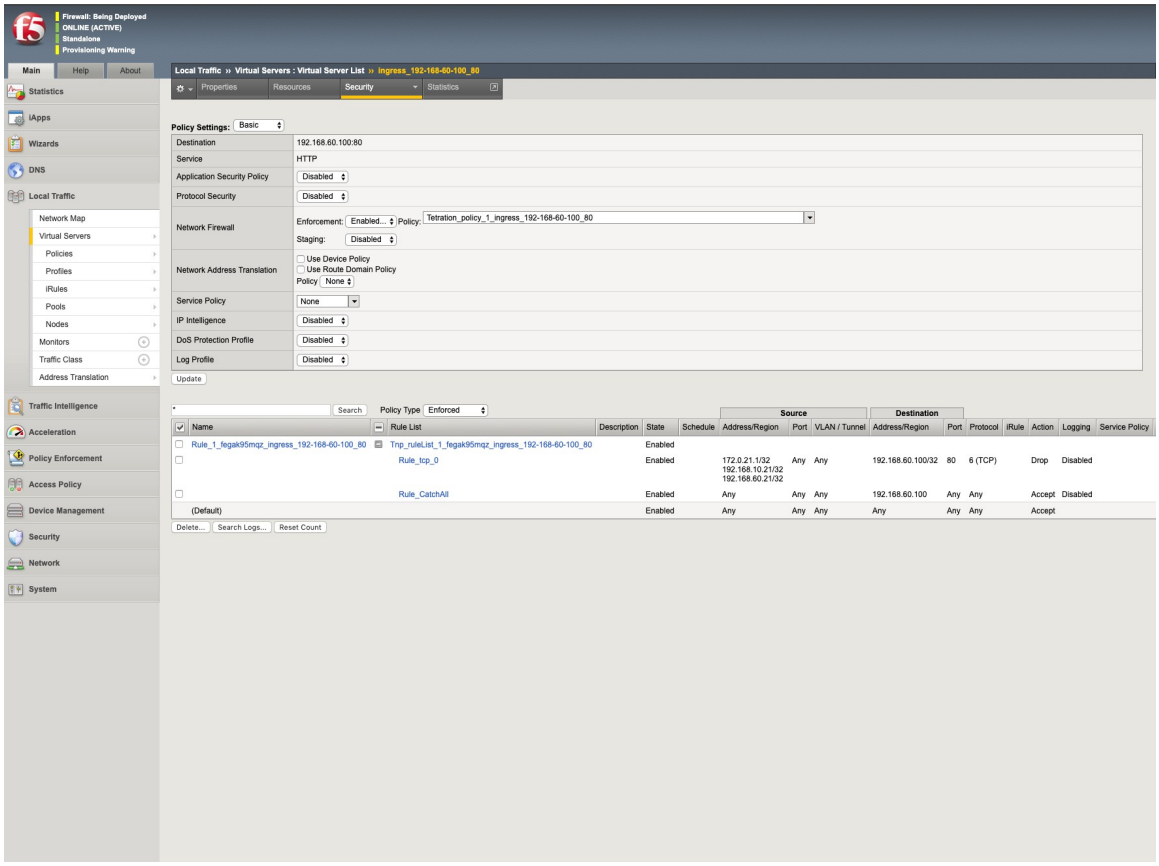
Étape 5 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accèdent. Dans l'exemple ci-dessous, nous avons créé un service *nginx* .

```
→  ~
→  ~ k8s get deploy
NAME    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
nginx   1         1         1            0           5s
→  ~
```

Étape 6 Créez une politique entre le consommateur externe et le service backend. Appliquez la politique à l'aide de l'onglet *Policy Enforcement* (Application des politiques).



Étape 7 Vérifiez les politiques sur l'équilibreur de charge *F5 BIG-IP* et les pods du backend. Dans le cas de F5, l'équilibreur de charge Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le consommateur spécifié à l'étape 6 et la destination sera la VIP [VIP du service virtuel Ingress pour F5]. Dans le cas de pods du serveur principal (backend), Cisco Secure Workload appliquera la règle autoriser/abandonner appropriée où la source sera le SNIP [dans le cas où le pool SNAT est activé] ou l'IP F5 [carte automatique activée] et la destination sera l'adresse IP du pod de backend.



Mises en garde

- Pendant la phase de déploiement du mode *F5 BIG-IP* HA, activez l'option *de synchronisation de la configuration* . Cela garantit que l'orchestrateur externe peut récupérer la dernière liste de serveurs virtuels auprès de l'hôte actuellement connecté.
- Dans le cas d'un mode de déploiement *F5 BIG-IP* HA, si la mise en correspondance *automatique* est configurée au lieu du regroupement SNAT pour la traduction d'adresses, assurez-vous que l'*adresse IP BIG-IP principale* est configurée avec l'adresse *Self IP* (Auto IP) flottante.
- Seule l'adresse VIP définie comme une adresse unique est prise en charge. L'adresse VIP donnée comme sous-réseau n'est pas prise en charge.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de *TaaS* , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez de privilèges d'accès en lecture et en écriture pour envoyer des requêtes d'API REST à l'appareil *F5 BIG-IP*.
- Règles de sécurité introuvables : Si aucune règle de sécurité n'est trouvée pour un serveur virtuel défini, après l'application de la politique, assurez-vous que le serveur virtuel correspondant est activé, c.-à-d. sa disponibilité/état doit être *disponible*/*activé*.

Citrix Netscaler

L'intégration Citrix Netscaler permet à Cisco Secure Workload d'importer les *serveurs virtuels d'équilibrage de la charge* à partir d'un dispositif d'équilibreur de charge Netscaler et d'en dériver des inventaires de services. Un inventaire de service correspond à un service Netscaler fourni par un serveur virtuel et possède des étiquettes telles que *service_name* (nom_service), qui peuvent être utilisées dans la recherche d'inventaire et pour créer des portées et des politiques pour Cisco Secure Workload.

Un des principaux avantages de cette fonctionnalité est l'application des politiques, car l'*orchestrateur externe pour Citrix Netscaler* traduit les politiques Cisco Secure Workload en règles de liste de contrôle d'accès Netscaler et les déploie sur l'équilibreur de charge Netscaler via son API REST.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Point terminal de l'API REST Netscaler version 12.0.57.19

Champs de configuration

En plus des champs de configuration courants, décrits dans la section*Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Liste d'hôtes	Oui	Ceci spécifie le point terminal de l'API REST pour l'équilibreur de charge Citrix Netscaler. Si la haute disponibilité est configurée sur Citrix Netscaler, saisissez un autre nœud membre de sorte qu'en cas de basculement, l'orchestrateur externe bascule sur le nœud actuel. Si vous souhaitez importer des étiquettes d'un autre équilibreur de charge Citrix Netscaler, créez un nouvel orchestrateur externe.
Activer l'application	Non	La valeur par défaut est faux (non cochée). Si cette option est cochée, cela permet Cisco Secure Workload *à l'application de la politique* de déployer les règles ACL sur l'équilibreur de charge Citrix Netscaler correspondant. Notez que les informations d'authentification fournies doivent autoriser un accès en écriture à l'API REST Citrix Netscaler.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST Netscaler est accessible à partir de la grappe Cisco Secure Workload.
- Pour le TaaS ou dans les cas où l'appareil Netscaler n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Créez un orchestrateur externe avec le type *Citrix Netscaler*.
- Selon la valeur de l' *intervalle* , cela peut prendre jusqu'à 60 secondes (intervalle par défaut) avant que le premier instantané complet des serveurs virtuels Netscaler ne se termine. Par la suite, les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.
- Appliquer les politiques de Cisco Secure Workload pour déployer les règles d'ACL Netscaler.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes pour un orchestrateur externe pour *Citrix Netscaler* :

Clé	Valeur
orchestrator_system/orch_type	nsbalancer
orchestrator_system/cluster_id	<UUID de l'orchestrateur externe>
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/workload_type	service
orchestrator_system/service_name	<Nom du serveur virtuel d'équilibrage de charge>

Étiquettes générées

Pour chaque serveur virtuel d'équilibrage de charge, l'orchestrateur externe génère les étiquettes suivantes :

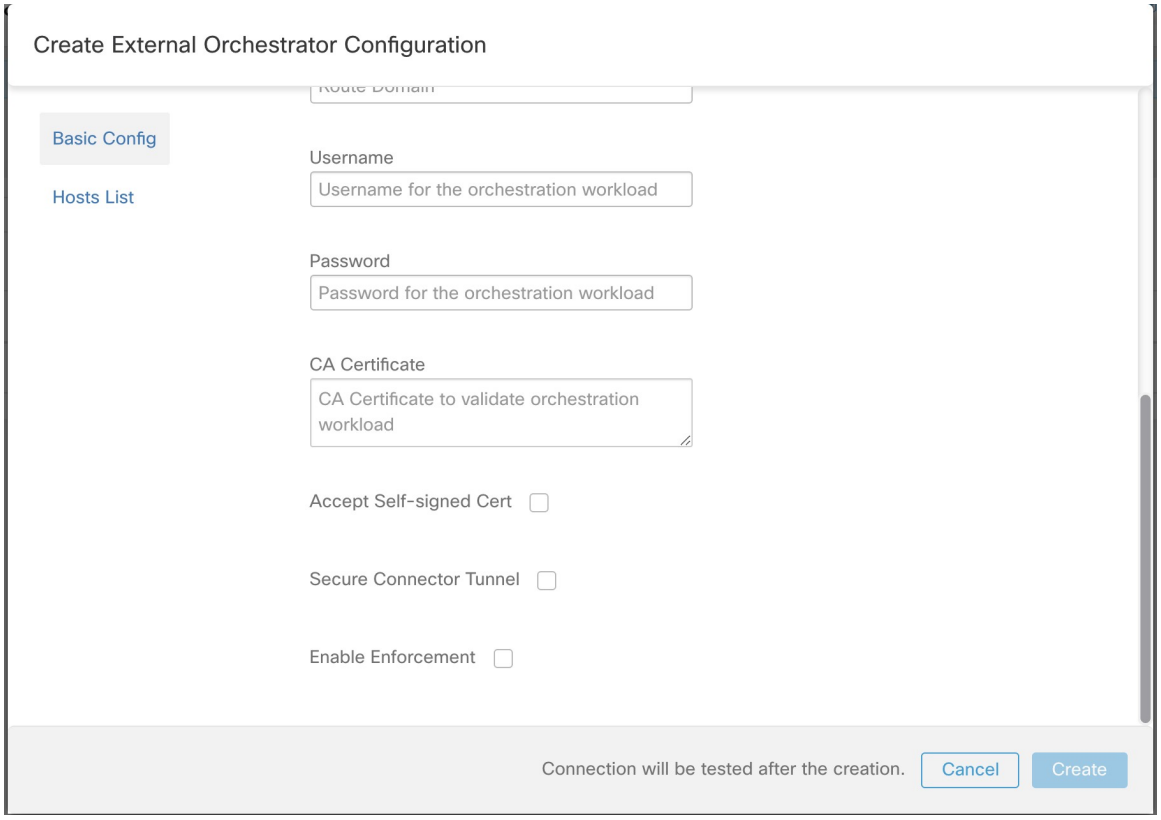
Clé	Valeur
orchestrator_annotation/snat_address	<Adresse SNAT des serveurs virtuels>

Application de la politique pour Citrix Netscaler

Cette fonctionnalité permet à Cisco Secure Workload de traduire les politiques logiques avec des groupes de fournisseurs qui correspondent aux serveurs virtuels étiquetés *Citrix Netscaler* en règles ACL *Citrix Netscaler* et de les déployer sur le dispositif de l'équilibreur de charge à l'aide de son API REST. Comme mentionné ci-dessus, toutes les règles ACL existantes seront remplacées par des règles de politique générées par Cisco Secure Workload.

Par défaut, le champ *Enable Enforcement* (Activer l'application) n'est pas coché. c'est à dire est désactivé, dans la boîte de dialogue *Create Orchestrator* (Créer un orchestrateur), comme le montre l'image ci-dessous :

Figure 57: Option de configuration « Enable Enforcement » (Activer l'application)

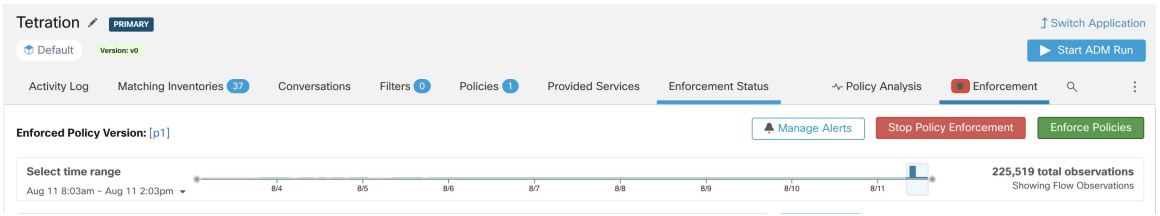


(Activer l'application)

Il suffit de cocher la case désignée pour activer l'application pour l'orchestrateur. Cette option peut être modifiée à tout moment au besoin.

Activer l'application pour l'orchestrateur, que cela se fasse en créant ou en modifiant la configuration de l'orchestrateur, ne déploiera pas immédiatement les politiques logiques actuelles sur le dispositif de l'équilibreur de charge. Cette tâche est effectuée dans le cadre de l'application de la politique d'espace de travail qui doit être déclenchée par l'utilisateur, comme le montre l'image suivante, ou en raison d'une mise à jour des inventaires. Cependant, la désactivation de l'application pour l'orchestrateur entraînera la suppression immédiate de toutes les règles ACL déployées de l'équilibreur de charge *Citrix Netscaler*.

Figure 58: Application des politiques de l'espace de travail



Note

- L'orchestrateur pour *Citrix Netscaler* détecte également tout écart par rapport aux règles ACL et le remplace par des politiques Cisco Secure Workload. Toute modification de politique à l'égard des serveurs virtuels d'équilibrage de charge doit être effectuée avec Cisco Secure Workload uniquement.
- Lorsque l'application des politiques est arrêtée ou que l'orchestrateur externe est supprimé, les listes de contrôle d'accès (ACL) deviennent vides, car toutes les politiques Cisco Secure Workload sont supprimées de l'équilibreur de charge *Citrix Netscaler*.

L'état d'application de la politique OpenAPI pour l'orchestrateur externe peut être utilisé pour récupérer l'état de l'application de la politique Cisco Secure Workload sur le dispositif de l'équilibreur de charge associé à l'orchestrateur externe. Cela permet de vérifier si le déploiement des règles ACL sur l'appareil *Citrix Netscaler* a réussi ou échoué.

Mises en garde

- Si l'application est activée, les politiques Cisco Secure Workload seront toujours déployées sur la liste globale des ACL, c.-à-d. *par défaut* de la partition.
- Seule l'adresse VIP définie comme une adresse unique est prise en charge. L'adresse VIP donnée comme modèle d'adresse n'est pas prise en charge.
- La visibilité des services détectés (serveurs virtuels *Citrix Netscaler*) n'est pas prise en charge.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de *TaaS* , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez de privilèges d'accès en lecture et en écriture pour envoyer des requêtes d'API REST à l'appareil *Citrix Netscaler*.
- Règles ACL introuvables. Si aucune règle ACL n'est trouvée, après l'application de la politique, assurez-vous que le serveur virtuel correspondant est activé, c.-à-d. son état doit être *opérationnel*.

TAXII

L'intégration TAXII (Trusted Automated Exchange of Intelligence Information) permet à Cisco Secure Workload d'acquérir les flux de données de renseignements sur les menaces des fournisseurs de sécurité pour annoter les flux réseau et les condensés de processus à l'aide d'indicateurs STIX (Structured Threat Information Expression) comme les adresses IP malveillantes, les condensés malveillants.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « taxii », l'appareil Cisco Secure Workload tente de se connecter au(x) serveur(s) TAXII et interroge les collections de flux de données STIX. Les flux de données STIX (uniquement les adresses IP et les indicateurs de condensé binaires) seront analysés

et utilisés pour annoter les flux réseau et les condensés de processus dans les pipelines de Cisco Secure Workload (comme appartenant au détenteur sous lequel l'orchestrateur est configuré).

Les flux réseau avec des adresses de fournisseur ou de consommateur correspondant à des adresses IP malveillantes importées seront étiquetés avec l'étiquette à valeurs multiples « orchestrator_malicious_ip_by_<nom du fournisseur> » où <nom du fournisseur> est l'entrée de configuration de l'orchestrateur d'utilisateur du fournisseur TAXII et la valeur de l'étiquette est « Yes » (Oui).

Les indicateurs de condensé binaire STIX intégrés seront utilisés pour annoter les condensés de processus de charge de travail, qui seront affichés (s'ils correspondent) dans le tableau de bord de sécurité et les détails de la note de condensé de processus, et dans le profil de charge de travail et condensés de fichier.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Serveurs TAXII pris en charge : 1.0
- Flux TAXII pris en charge avec la version STIX : 1.x

Champs de configuration

En plus des champs de configuration courants, décrits dans la section*Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Nom	Oui	Nom de l'orchestrateur spécifié par l'utilisateur.
Description	Oui	Description de l'orchestrateur précisée par l'utilisateur.
Fournisseur	Oui	Le fournisseur fournit les flux de données de renseignements.
Intervalle complet entre les instantanés	Oui	L'intervalle (en secondes) pour effectuer un instantané complet du flux TAXII. (Par défaut : 1 jour)
URL de l'interrogation	Oui	Le chemin d'accès complet de l'URL d'interrogation pour interroger les données.
Collecte	Oui	Le nom de la collecte de flux TAXII à interroger.
Jours d'interrogation	Oui	Le nombre de données sur les menaces de jours antérieurs à interroger à partir du flux TAXII.

Champs communs	Obligatoire	Description
Nom d'utilisateur		Nom d'utilisateur pour l'authentification.
Mot de passe		Mot de passe d'authentification.
Certificat		Votre certificat client servira à l'authentification.
Clé		Clé correspondant au certificat client.
Certificat de l'autorité de certification		Certificat de l'autorité de certification pour valider le point terminal de l'orchestration.
Accept Self-signed Cert (Accepter le certificat autosigné)		Case pour désactiver la vérification strictSSL du certificat du serveur d'API TAXII certificat
Secure Connector Tunnel (Tunnel du connecteur sécurisé)		Connexions de tunnel vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel du connecteur sécurisé.
Liste d'hôtes	Oui	Les paires nom d'hôte/adresse IP et la paire de ports pointant vers le ou les serveurs TAXII.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur TAXII est accessible sur cette adresse IP ou ce port à partir de la grappe Cisco Secure Workload.
- Configurez le serveur TAXII adéquat avec le chemin d'interrogation et le nom du flux TAXII.

Étiquettes générées

Clé	Valeur
orchestrator_system/orch_type	*TAXII*
orchestrator_system/cluster_id	L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload.
orchestrator_system/cluster_name	Nom donné à la configuration de cette grappe>.

Clé	Valeur
orchestrator_malicious_ip_by_ <vendor>	*Yes (Oui)* , si l'adresse du fournisseur ou du client de flux correspond aux données d'adresses IP malveillantes TAXII importées.

Mises en garde

- L'intégration de TAXII est prise en charge uniquement sur Cisco Secure Workload sur site.
- Seuls les adresses IP et les indicateurs de condensé des flux TAXII font l'objet d'une intégration.
- Le nombre maximal d'adresses IP intégrées est de 100 K (dernière mise à jour) par flux TAXII.
- Le nombre maximal de condensés intégrés est de 500 K (dernière mise à jour) pour tous les flux TAXII.
- Seuls les flux TAXII avec STIX version 1.x sont pris en charge.

Dépannage

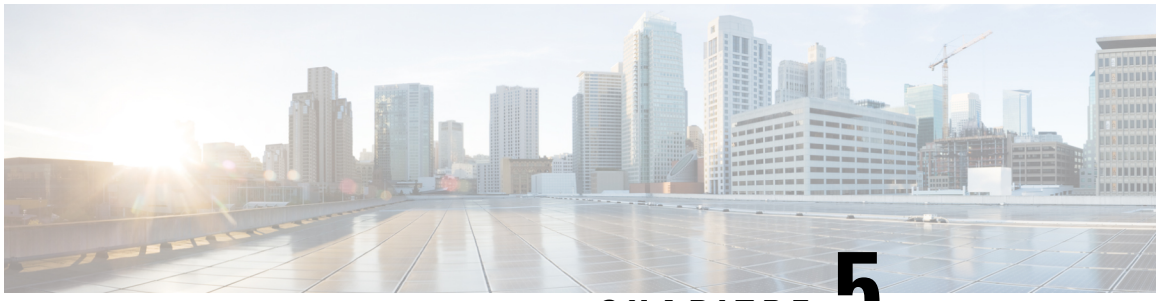
- Problèmes de connexion

  Le Cisco Secure Workload tentera de se connecter au chemin d'URL d'interrogation fourni à partir de l'un des Cisco Secure Workload serveurs d'appareils ou de la machine virtuelle qui héberge le service de tunnel VPN du connecteur sécuriséCisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic.

Comportement de l'interrogation complète pour les orchestrateurs TAXII

L'intervalle par défaut des instantanés complets est de 24 heures

À chaque intervalle d'instantané complet, Cisco Secure Workload extrait les flux TAXII des adresses IP et des condensés de fichiers jusqu'aux limites ci-dessus dans la base de données d'étiquettes.



CHAPITRE 5

Configurer et gérer les connecteurs pour Cisco Secure Workload

Les connecteurs permettent à Cisco Secure Workload de s'intégrer à des ressources externes, telles que les commutateurs réseau, les routeurs, les pare-feu et les systèmes de gestion des terminaux, pour recueillir des données de télémétrie, acquérir des observations de flux et élargir le contexte de l'inventaire et des terminaux.

Que sont les connecteurs

Les connecteurs de Cisco Secure Workload sont des intégrations qui permettent à Cisco Secure Workload d'interagir avec diverses ressources et de recueillir des données à partir de diverses ressources à des fins différentes. Pour configurer et utiliser les connecteurs, dans le volet de navigation, choisissez **Manage (Gestion)** > **Connectors (Connecteurs)**.

Note Les connecteurs nécessitent une appliance virtuelle. Pour en savoir plus, consultez la section Appliances virtuelles pour les connecteurs.

Connecteurs pour l'acquisition de flux

Les connecteurs transmettent les observations de flux de différents commutateurs de réseau, routeurs et autres boîtiers intermédiaires (tels que les équilibreurs de charge et les pare-feu) à Cisco Secure Workload à des fins d'acquisition de flux.

Cisco Secure Workload prend en charge l'acquisition de flux par l'intermédiaire de NetFlow v9, IPfIX et des protocoles personnalisés. En plus des observations des flux, les connecteurs de boîtier intermédiaire relient les flux côté client et côté serveur pour comprendre quels flux client sont liés à quels flux serveur.

Connecteur	Description	Déployé sur une appliance virtuelle
NetFlow	Recueillez les données télémétriques NetFlow V9 ou IP-fIX à partir d'appareils réseau comme les routeurs et les commutateurs.	Acquisition de Cisco Secure Workload
F5 BIG-IP	Recueillez les données télémétriques de F5 BIG-IP, reliez les flux côté client et côté serveur, et enrichissez l'inventaire du client avec les attributs utilisateur.	Acquisition de Cisco Secure Workload
Citrix Netscaler	Recueillez la télémétrie de Citrix ADC, reliez des flux côté client et côté serveur.	Acquisition de Cisco Secure Workload
Pare-feu du connecteur sécurisé Cisco	Recueillez les données de télémétrie à partir de Cisco Secure Firewall ASA, de Cisco Secure Firewall Threat Defense, et reliez les flux côté client et côté serveur.	Acquisition de Cisco Secure Workload
Meraki	Recueillez les données de télémétrie des pare-feux Meraki.	Acquisition de Cisco Secure Workload
ERSPAN	Recueillir les données de télémétrie ERSPAN à partir de périphériques réseau qui prennent en charge ERSPAN	Acquisition de Cisco Secure Workload
Consultez aussi	connecteurs infonuagiques	–

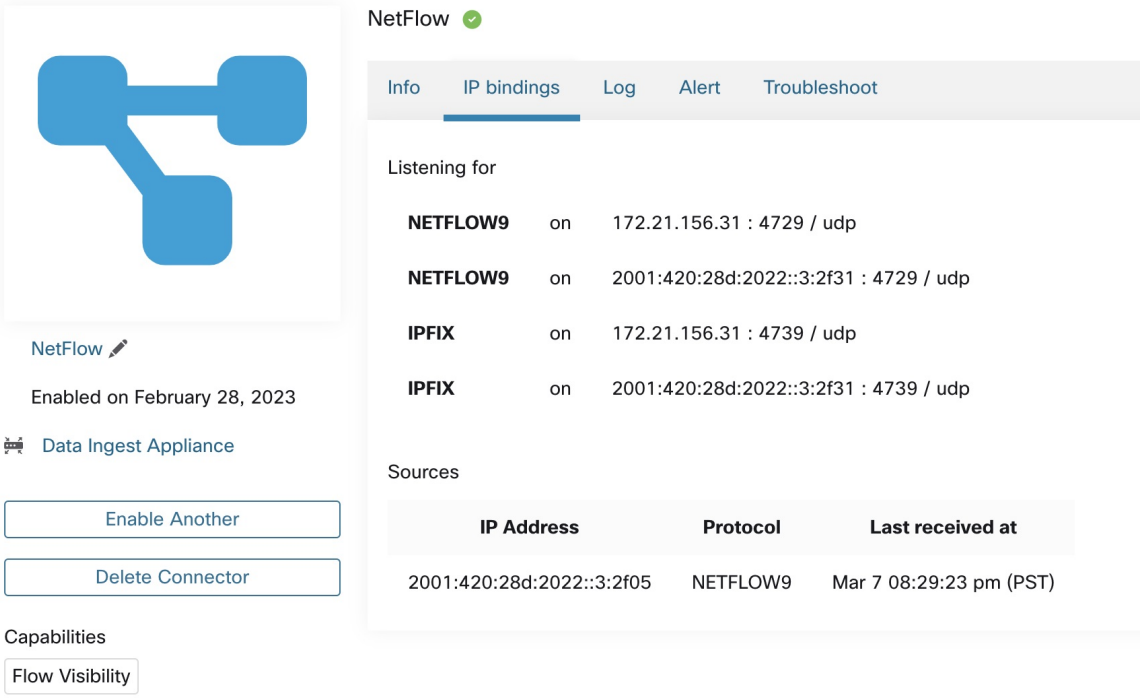
Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

Connecteur NetFlow

Le connecteur NetFlow permet à Cisco Secure Workload d'intégrer les observations de flux des routeurs et des commutateurs du réseau.

Cette solution permet aux hôtes d'éviter d'exécuter des agents logiciels, car les commutateurs Cisco relayent les enregistrements NetFlow à un connecteur NetFlow hébergé dans un appareil d'acquisition Cisco Secure Workload pour traitement.

Figure 59: Connecteur NetFlow



Qu'est-ce que NetFlow

Le protocole NetFlow permet aux routeurs et aux commutateurs d'agréger le trafic qui les traverse en flux et d'exporter ces flux vers un collecteur de flux.

Le collecteur de flux reçoit ces enregistrements de flux et les stocke pour les interroger et les analyser hors ligne. Les routeurs et commutateurs Cisco prennent en charge NetFlow.

En règle générale, la configuration comprend les étapes suivantes :

1. Activez la fonctionnalité NetFlow sur un ou plusieurs périphériques réseau et configurez les modèles de flux que les périphériques doivent exporter.
2. Configurez les informations de point terminal du collecteur NetFlow sur les périphériques réseau distants. Ce collecteur NetFlow est à l'écoute sur le point terminal configuré pour recevoir et traiter les enregistrements de flux NetFlow.

Acquisition de flux dans Cisco Secure Workload

Le connecteur NetFlow est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements de flux des périphériques réseau et les transfère à Cisco Secure Workload pour une analyse du flux. Vous pouvez activer un connecteur NetFlow sur un appareil d'acquisition Cisco Secure Workload et l'exécuter en tant que conteneur Docker.

Le connecteur NetFlow s'enregistre également auprès de Cisco Secure Workload en tant qu'agent NetFlow Cisco Secure Workload. Le connecteur NetFlow désencapsule les paquets de protocole NetFlow (c'est-à-dire les enregistrements de flux); traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Remarque Le connecteur NetFlow prend en charge les protocoles NetFlow v9 et IPFIX.

Remarque Chaque connecteur NetFlow ne doit signaler les flux que pour un seul VRF. Le connecteur exporte les flux et les place dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Secure Workload.

Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* (Configurations VRF à distance de l'agent), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur.

Le formulaire vous demande de fournir : le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Limitation de débit

Le connecteur NetFlow accepte jusqu'à 15 000 flux par seconde. Notez qu'un paquet NetFlow v9 ou IPFIX peut contenir un ou plusieurs enregistrements de flux et de modèle. Le connecteur NetFlow analyse les paquets et identifie les flux. Si le connecteur analyse plus de 15 000 flux par seconde, il abandonne les enregistrements de flux supplémentaires.

Notez également que le client Cisco Secure Workload ne prend en charge le connecteur NetFlow que si le débit se trouve dans cette limite acceptable.

Si le débit dépasse 15 000 flux par seconde, nous vous recommandons de commencer par régler le débit pour qu'il respecte les limites et de maintenir ce niveau pendant au moins trois jours (pour exclure les problèmes liés à un débit entrant plus élevé).

Si le problème persiste, le service d'assistance à la clientèle commence à examiner le problème et à identifier une solution de contournement et/ou une solution appropriée.

Éléments d'information pris en charge

Le connecteur NetFlow prend *uniquement* en charge les éléments d'information suivants dans les protocoles NetFlow v9 et IPFIX. Pour en savoir plus, consultez Entités IP Flow Information Export (IPFIX).

ID d'élément	Nom	Description	Obligatoire
1	octetDeltaCount	Nombre d'octets dans les paquets entrants pour ce flux.	Oui
2	packetDeltaCount	Nombre de paquets entrants pour ce flux.	Oui
4	protocolIdentifier	Valeur du numéro de protocole de l'en-tête du paquet IP.	Oui

ID d'élément	Nom	Description	Obligatoire
6	tcpControlBits	Bits de commande TCP observés pour les paquets de ce flux. L'agent gère les indicateurs FIN, SYN, RST, PSH, ACK et URG.	Non
7	sourceTransportPort	Identifiant du port source dans l'en-tête de transport.	Oui
8	sourceIPv4Address	Adresse source IPv4 dans l'en-tête du paquet IP.	8 ou 27
11	destinationTransportPort	Identifiant du port de destination dans l'en-tête de transport.	Oui
12	destinationIPv4Address	Adresse de destination IPv4 dans l'en-tête du paquet IP.	12 ou 28
27	sourceIPv6Address	Adresse source IPv6 dans l'en-tête du paquet IP.	8 ou 27
28	destinationIPv6Address	Adresse de destination IPv6 dans l'en-tête du paquet IP.	12 ou 28
150	flowStartSeconds	Horodatage absolu du premier paquet du flux (en secondes).	Non
151	flowEndSeconds	Horodatage absolu du dernier paquet du flux (en secondes).	Non
152	flowStartMilliseconds	Horodatage absolu du premier paquet du flux (en millisecondes).	Non
153	flowEndMilliseconds	Horodatage absolu du dernier paquet du flux (en millisecondes).	Non
154	flowStartMicroseconds	Horodatage absolu du premier paquet du flux (en microsecondes).	Non
155	flowEndMicroseconds	Horodatage absolu du dernier paquet du flux (en microsecondes).	Non

ID d'élément	Nom	Description	Obligatoire
156	flowStartNanoseconds	Horodatage absolu du premier paquet du flux (en nanosecondes).	Non
157	flowEndNanoseconds	Horodatage absolu du dernier paquet du flux (en nanosecondes).	Non

Comment configurer NetFlow sur le commutateur

Les étapes suivantes concernent un commutateur Nexus 9000. Les configurations peuvent différer légèrement pour les autres plateformes Cisco. Dans tous les cas, consultez le guide de configuration officiel de Cisco pour la plateforme Cisco que vous configurez.

Procedure

Étape 1 Entrer en mode de configuration globale.

```
switch# configure terminal
```

Étape 2 Activez la fonction NetFlow.

```
switch(config)# feature netflow
```

Étape 3 Configurez un enregistrement de flux.

L'exemple de configuration suivant montre comment générer des informations de cinq tuples d'un flux dans un enregistrement NetFlow.

```
switch(config)# flow record ipv4-records
switch(config-flow-record)# description IPv4Flow
switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match transport source-port
switch(config-flow-record)# match transport destination-port
switch(config-flow-record)# collect transport tcp flags
switch(config-flow-record)# collect counter bytes
switch(config-flow-record)# collect counter packets
```

Étape 4 Configurez un exportateur de flux.

L'exemple de configuration suivant précise la version du protocole NetFlow, l'intervalle d'échange du modèle NetFlow et les détails de point de terminaison du collecteur NetFlow. Préciser l'adresse IP et le port sur lesquels vous activez le connecteur NetFlow sur un appareil d'acquisition Cisco Secure Workload.

```
switch(config)# flow exporter flow-exporter-one
switch(config-flow-exporter)# description NetFlowv9ToNetFlowConnector
switch(config-flow-exporter)# destination 172.26.230.173 use-vrf management
switch(config-flow-exporter)# transport udp 4729
switch(config-flow-exporter)# source mgmt0
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# template data timeout 20
```

Étape 5 Configurez un moniteur de flux.

Créez un moniteur de flux et associez-le à un enregistrement de flux et à un exportateur de flux.

```
switch(config)# flow monitor ipv4-monitor
switch(config-flow-monitor)# description IPv4FlowMonitor
switch(config-flow-monitor)# record ipv4-records
switch(config-flow-monitor)# exporter flow-exporter-one
```

Étape 6 appliquez le moniteur de flux à une interface.

```
switch(config)# interface Ethernet 1/1
switch(config-if)# ip flow monitor ipv4-monitor input
```

Les étapes ci-dessus configurent NetFlow sur le Nexus 9000 pour exporter les paquets de protocole NetFlow v9 pour le trafic entrant passant par l'interface 1/1. Il envoie les enregistrements de flux au 172.26.230.173:4729 sur un protocole UDP. Chaque enregistrement de flux comprend des informations de cinq tuples du trafic et le nombre d'octets/paquets du flux.

Figure 60: Configuration d'exécution de NetFlow sur le commutateur Cisco Nexus 9000

```
switch# show running-config netflow

!Command: show running-config netflow
!Time: Wed Mar 21 04:25:21 2018

version 7.0(3)I7(1)
feature netflow

flow timeout 60
flow exporter flow-exporter-173
  destination 172.26.230.173 use-vrf management
  transport udp 4729
  source mgmt0
  version 9
    template data timeout 20
flow record ipv4-records
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match transport source-port
  match transport destination-port
  collect transport tcp flags
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
flow monitor ipv4-monitor
  record ipv4-records
  exporter flow-exporter-173


interface Ethernet1/1
  ip flow monitor ipv4-monitor input

interface Ethernet1/2
  ip flow monitor ipv4-monitor input

switch#
```

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Pour les connecteurs NetFlow, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs NetFlow sur un seul appareil d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs NetFlow sur un détenteur (portée racine)	10
Nombre maximal de connecteurs NetFlow sur Cisco Secure Workload	100

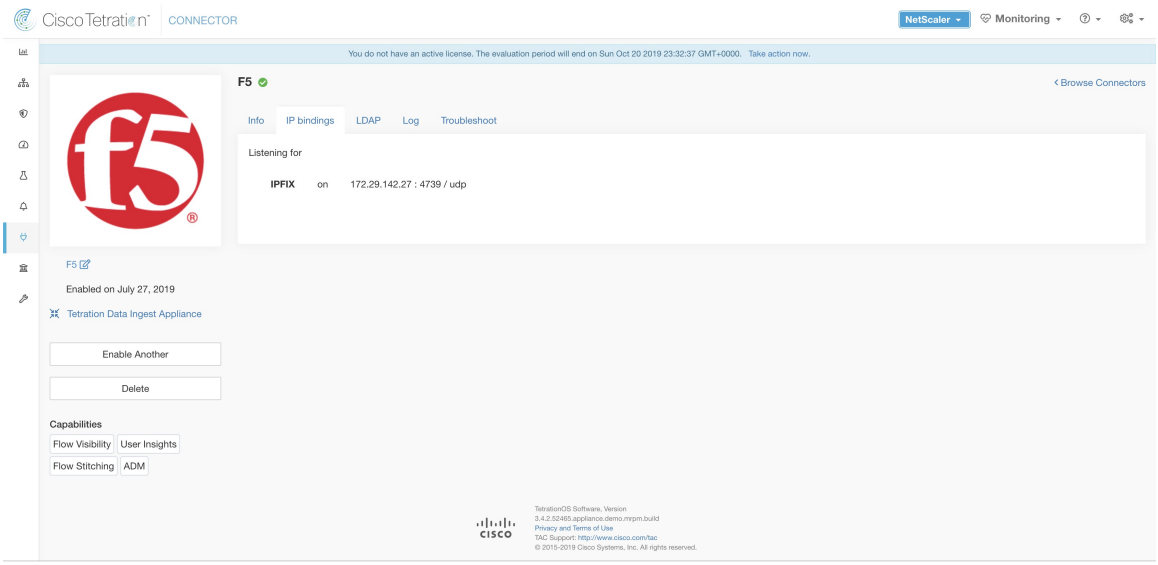
Connecteur F5

Le connecteur F5 permet à Cisco Secure Workload d'acquérir les observations de flux ADC F5 BIG-IP.

Il permet à Cisco Secure Workload de surveiller à distance les observations de flux sur les ADC F5 BIG-IP, d'assembler les flux côté client et côté serveur et d'annoter les utilisateurs sur les adresses IP clients (si les informations sur les utilisateurs sont disponibles).

Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les ADC F5 BIG-IP configurent l'exportation des enregistrements IPFIXvers le connecteur F5 pour traitement.

Figure 61: Connecteur F5



What is F5 BIG-IP IPFIX

F5 BIG-IP IPFIX logging collects flow data for traffic going through the F5 BIG-IP and exports IPFIX records to flow collectors.

Typically, the setup involves the following steps:

1. Create IPFIX Log-Publisher on F5 BIG-IP appliance.
2. Configure the IPFIX Log-Destination on the F5 BIG-IP appliance. This log-destination will be listening on configured endpoint to receive and process flow records.
3. Create an F5 iRule that publishes IPFIX flow records to the log-publisher.
4. Add the F5 iRule to the virtual server of interest.

Note F5 connector supports F5 BIG-IP software version 12.1.2 and above.

Acquisition de flux dans Cisco Secure Workload

Le connecteur F5 BIG-IP est principalement un collecteur IPFIX. Le connecteur reçoit les enregistrements de flux des CAN F5 BIG-IP, connecte les flux avec NAT et les transfère à Cisco Secure Workload pour une analyse des flux. En outre, si la configuration LDAP est fournie au connecteur F5, il détermine les valeurs des attributs LDAP configurés d'un utilisateur associé à la transaction (si F5 authentifie l'utilisateur avant de traiter la transaction). Les attributs sont associés à l'adresse IP du client où le flux s'est produit.

Remarque Le connecteur F5 prend uniquement en charge le protocole IPFIX.

Remarque Chaque connecteur F5 ne signale les flux que pour un VRF. Le connecteur place les flux qu'il exporte dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Cisco Secure Workload.

Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* (Configurations VRF à distance de l'agent), cliquez sur l'onglet *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire vous demande de fournir : le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

How to configure IPFIX on F5 BIG-IP

The following steps are for F5 BIG-IP load balancer. (Ref: Configuring F5 BIG-IP for IPFIX)

Purpose	Description
1. Create a pool of IPFIX collectors.	On F5 BIG-IP appliance, create the pool of IPFIX collectors. These are the IP addresses associated with F5 connectors on a Cisco Secure Workload Ingest appliance. F5 connectors run in Docker containers on the VM listen on port 4739 for IPFIX packets.
2. Create a log-destination.	The log destination configuration on F5 BIG-IP appliance specifies the actual pool of IPFIX collectors that should be used.
3. Create a log-publisher.	A log publisher specifies where F5 BIG-IP sends the IPFIX messages. The publisher is bound with a log-destination.
4. Add a F5 and Cisco Secure Workload approved iRule.	Secure Workload and F5 developed iRules that will export flow records to F5 connectors. These iRules will export complete information about a given transaction: including all the endpoints, byte and packet counts, flow start and end time (in milliseconds). F5 connectors will create 4 independent flows and match each flow with its related flow.
5. Add the iRule to the virtual server.	In the iRule settings of a virtual server, add the Secure Workload, approved iRule to the virtual server.

The above steps configures IPFIX on F5 BIG-IP load balancer to export IPFIX protocol packets for traffic going through the appliance. Here is a sample config of F5.

Figure 62: Running configuration of IPFIX on F5 BIG-IP load balancer

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm  pool ipfix-pool-1
ltm pool ipfix-pool-1 {
    members {
        10.28.118.6:ipfix {
            address 10.28.118.6
            session monitor-enabled
            state up
        }
    }
    monitor gateway_icmp
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config sys  log-config
sys log-config destination ipfix ipfix-collector-1 {
    pool-name ipfix-pool-1
    transport-profile udp
}
sys log-config publisher ipfix-pub-1 {
    destinations {
        ipfix-collector-1 { }
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

In the example above, flow records will be published to *ipfix-pub-1*. *ipfix-pub-1* is configured with log-destination *ipfix-collector-1* which sends the IPFIX messages to IPFIX pool *ipfix-pool-1*. *ipfix-pool-1* has 10.28.118.6 as one of the IPFIX collectors. The virtual server *vip-1* is configured with IPFIX iRule *ipfix-rule-1* which specifies the IPFIX template and how the template gets filled and sent.

- F5 and Cisco Secure Workload approved iRule for TCP virtual server can be found in the following file See L4 iRule for TCP virtual server.

F5 and Cisco Secure Workload approved iRule for UDP virtual server can be found in the following file.

- See L4 iRule for UDP virtual server.

F5 and Cisco Secure Workload approved iRule for HTTPS virtual server with authentication enabled can be found in the following file.

- See iRule for HTTPS virtual server.

Note Before using the iRule downloaded from this guide, please update the **log-publisher** to point to the log-publisher configured in the F5 connector where the iRule will be added.

Note F5 has published a GitHub repository, f5-tetration to help users get started with flow-stitching. The iRules for publishing IPFIX records to F5 connector for various protocol types are available at: f5-tetration/irules. Please visit this site for latest iRule definitions. In addition, F5 also developed a script to: (1) install the correct iRule for the virtual servers, (2) add a pool of IPFIX collector endpoints (where F5 connectors listen for IPFIX records), (3) configure the log-collector and log-publisher, and (4) bind the correct iRule to the virtual servers. This tool minimizes manual configuration and user error while enabling flow-stitching use-case. The script is available at f5-tetration/scripts.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs.

Les configurations suivantes sont autorisées sur le connecteur.

- LDAP : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour choisir l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

En outre, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande qui peut être exécutée sur le conteneur. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

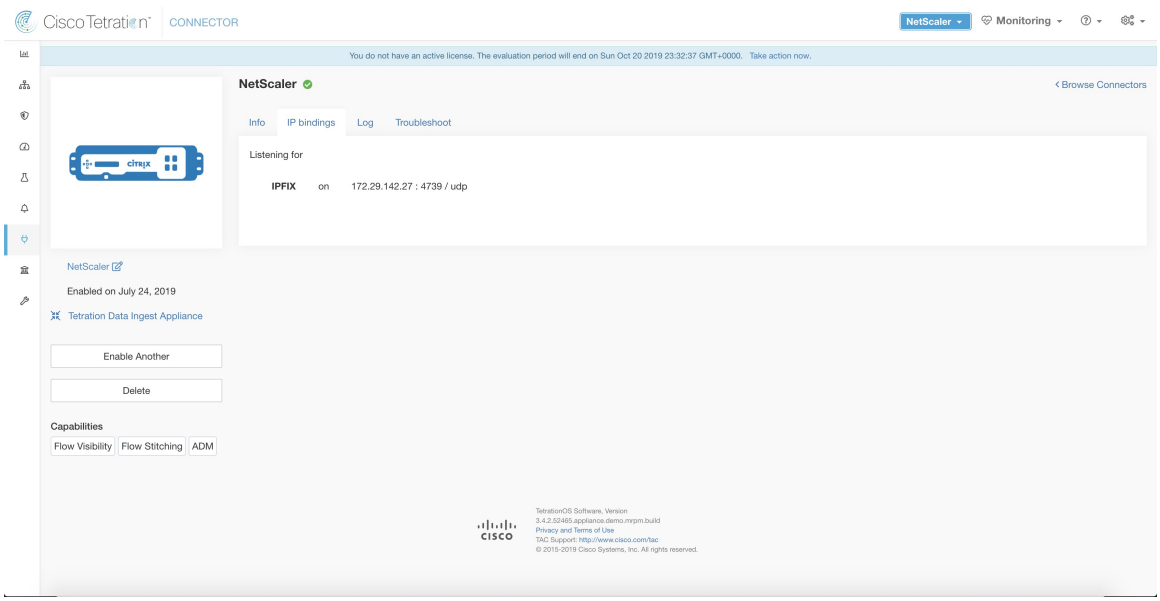
Limites

Unité	Limite
Nombre maximal de connecteurs F5 sur un dispositif d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs F5 sur un détenteur (portée racine)	10
Nombre maximal de connecteurs F5 sur Cisco Secure Workload	100

Connecteur NetScaler

Le connecteur NetScaler permet à Cisco Secure Workload d'acquérir les observations de flux des ADC Citrix (Citrix NetScalers). Il permet à Cisco Secure Workload de surveiller à distance les observations de flux sur les ADC Citrix et d'assembler les flux côté client et côté serveur. Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les ADC Citrix sont configurés pour exporter les enregistrements IPfFIX vers le connecteur NetScaler pour traitement.

Figure 63: Connecteur NetScaler



What is Citrix NetScaler AppFlow

Citrix NetScaler AppFlow collects flow data for traffic going through the NetScaler and exports IPFIX records to flow collectors. Citrix AppFlow protocol uses IPFIX to export the flows to flow collectors. Citrix AppFlow is supported in Citrix NetScaler load balancers.

Typically, the setup involves the following steps:

1. Enable AppFlow feature on one or more Citrix NetScaler instances.
2. Configure the AppFlow collector endpoint information on the remote network devices. This AppFlow collector will be listening on configured endpoint to receive and process flow records.
3. Configure AppFlow actions and policies to export flow records to AppFlow collectors.

Note NetScaler connector supports Citrix ADC software version 11.1.51.26 and above.

Acquisition de flux dans Cisco Secure Workload

Le connecteur NetScaler est essentiellement un collecteur Citrix AppFlow (IPFIX). Le connecteur reçoit les enregistrements de flux des ADC Citrix, regroupe les flux avec NAT et les transfère à Cisco Secure Workload pour une analyse des flux. Un connecteur NetScaler peut être activé sur un appareil d'acquisition Cisco Cisco Secure Workload et s'exécute en tant que conteneur Docker. Le connecteur NetScaler s'enregistre également auprès de Cisco Secure Workload en tant qu'agent NetScaler Cisco Secure Workload.

Note Le connecteur NetScaler prend uniquement en charge le protocole IPFIX.

Note Chaque connecteur NetScaler ne doit signaler les flux que pour un seul VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet Configuration. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

How to configure AppFlow on NetScaler

The following steps are for NetScaler load balancer. (Ref: Configuring AppFlow)

Procedure

Étape 1 Enable AppFlow on NetScaler.

```
enable ns feature appflow
```

Étape 2 Add AppFlow collector endpoints.

The collector receives the AppFlow records from NetScaler. Please specify the IP and port of NetScaler connector enabled on a Cisco Secure Workload Ingest appliance as an AppFlow collector.

```
add appflow collector c1 -IPAddress 172.26.230.173 -port 4739
```

Étape 3 Configure an AppFlow action.

This lists the collectors that will get AppFlow records if the associated AppFlow policy matches.

```
add appflow action a1 -collectors c1
```

Étape 4 Configure an AppFlow policy.

This is a rule that has to match for an AppFlow record to be generated.

```
add appflow policy p1 CLIENT.TCP.DSTPORT(22) a1
add appflow policy p2 HTTP.REQ.URL.SUFFIX.EQ("jpeg") a1
```

Étape 5 Bind AppFlow policy to Virtual Server.

Traffic hitting the IP of the virtual server (VIP) will be evaluated for AppFlow policy matches. On a match, a flow record is generated and sent to all collectors listed in the associated AppFlow action.

```
bind lb vserver lb1 -policyname p1 -priority 10
```

Étape 6 Optionally, bind AppFlow policy globally (for all virtual servers).

An AppFlow policy could also be bound globally to all virtual servers. This policy applies to all traffic that flows through Citrix ADC.

```
bind appflow global p2 1 NEXT -type REQ_DEFAULT
```

Étape 7 Optionally, template refresh interval.

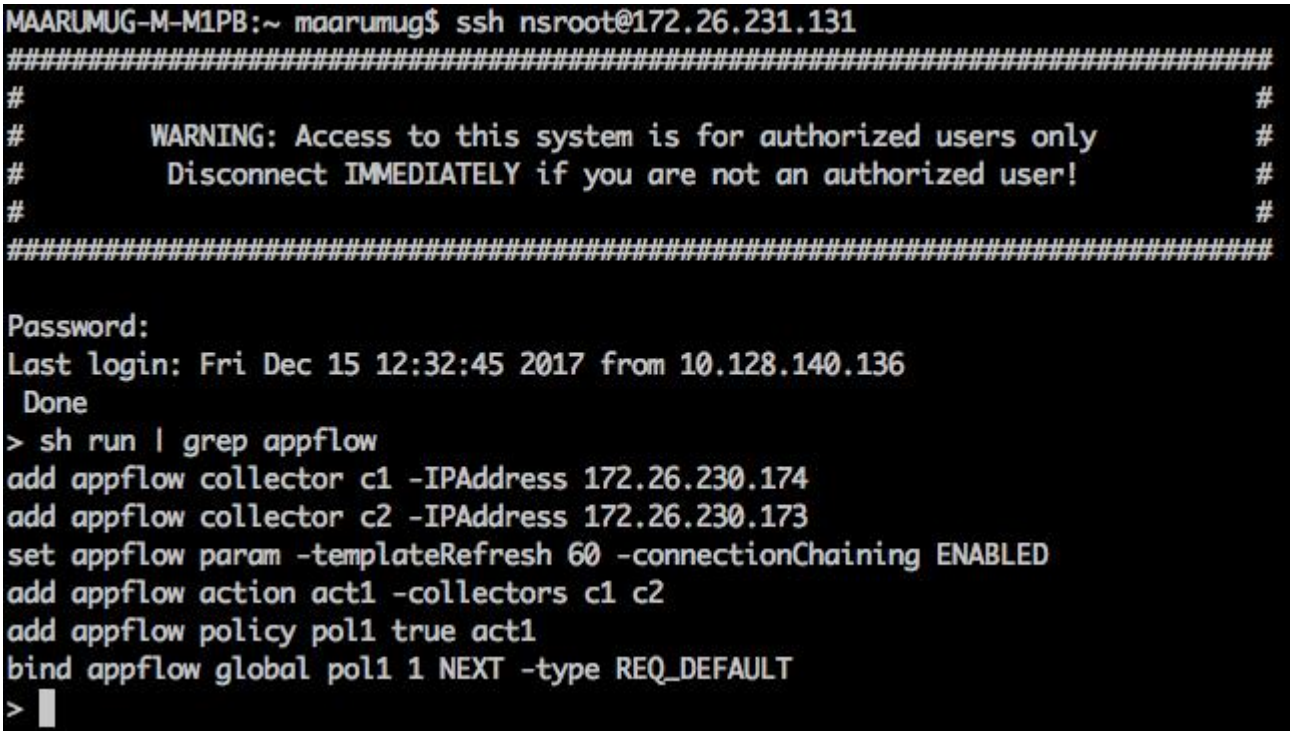
Default value for template refresh is 60 seconds.

```
set appflow param -templatereferesh 60
```

The above steps configures AppFlow on Citrix NetScaler load balancer to export IPFIX protocol packets for traffic going through NetScaler. The flow records will be sent to either 172.26.230.173:4739 (for traffic going through vserver lb1) and to 172.26.230.184:4739 (for all traffic going through the NetScaler). Each flow record includes 5 tuple information of the traffic and the byte/packet count of the flow.

The following screenshot shows a running configuration of AppFlow on a Citrix NetScaler load balancer.

Figure 64: Running configuration of AppFlow on Citrix NetScaler load balancer



Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour

et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. . Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

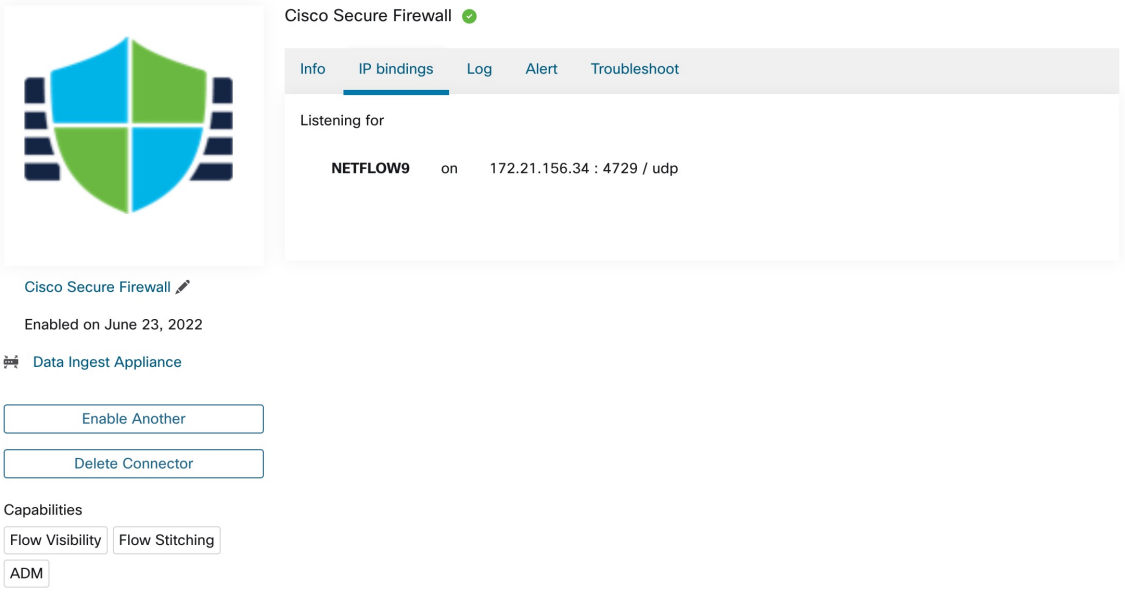
Tableau 17 : Limites

Unité	Limite
Nombre maximal de connecteurs NetScaler sur un appareil d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs NetScaler sur un détenteur (portée racine)	10
Nombre maximal de connecteurs NetScaler sur Cisco Secure Workload	100

Cisco Secure Firewall Connector

Secure Firewall Connector (formerly known as ASA Connector) allows Cisco Secure Workload to ingest flow observations from Secure Firewall ASA (formerly known as Cisco ASA) and Secure Firewall Threat Defense (formerly known as Firepower Threat Defense or FTD). Using this solution, the hosts do not need to run software agents, because the Cisco switches will relay NetFlow Secure Event Logging (NSEL) records to Secure Firewall Connector hosted in a Cisco Secure Workload Ingest appliance for processing.

Figure 65: Secure Firewall Connector



Cisco Secure Firewall ASA NetFlow Secure Event Logging (NSEL) provides a stateful, IP flow monitoring that exports significant events in a flow to a NetFlow collector. When an event causes a state change on a

flow, an NSEL event is triggered that sends the flow observation along with the event that caused the state change to the NetFlow collector. The flow collector receives these flow records and stores them in their flow storage for offline querying and analysis.

Typically, the setup involves the following steps:

1. Enable NSEL feature on Secure Firewall ASA and/or Secure Firewall Threat Defense.
2. Configure the Secure Firewall connector endpoint information on Secure Firewall ASA and/or Secure Firewall Threat Defense. Secure Firewall connector will be listening on configured endpoint to receive and process NSEL records.

Acquisition de flux dans Cisco Secure Workload

Le connecteur de Cisco Secure Firewall est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements NSEL de Cisco Secure Firewall ASA et de Cisco Secure Firewall Threat Defense et les transmet à Cisco Secure Workload pour analyse du flux. Le connecteur de Cisco Secure Firewall peut être activé sur un appareil d'acquisition Cisco Secure Workload et s'exécute en tant que conteneur Docker.

Le connecteur de Cisco Secure Firewall s'enregistre également auprès de Cisco Secure Workload en tant qu'agent Cisco Secure Workload. Le connecteur de Cisco Secure Firewall désencapsule les paquets de protocole NSEL (c.-à-d. les enregistrements de flux). traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Note Le connecteur de Cisco Secure Firewall prend en charge le protocole NetFlow v9.

Note Chaque connecteur Cisco Secure Firewall ne doit signaler les flux que pour un seul VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Gestion des événements NSEL

Le tableau suivant montre comment les divers événements NSEL sont gérés par le connecteur Secure Firewall. Pour en savoir plus sur ces éléments, consultez le document Entités d'exportation d'informations sur les flux IP (IPFIX).

ID de l'élément de l'événement de flux : 233 Nom de l'élément : *NF_F_FW_EVENT*	Événement de flux étendu ID de l'élément : 33002 Nom de l'élément : *NF_F_FW_EXT_EVENT*	Action sur le connecteur de Cisco Secure Firewall
0 (par défaut, ignorez cette valeur)	Ce n'est pas important	Aucune opération
1 (Flux créé)	Ce n'est pas important	Envoyer le flux à Cisco Secure Workload

ID de l'élément de l'événement de flux : 233 Nom de l'élément : *NF_F_FW_EVENT*	Événement de flux étendu ID de l'élément : 33002 Nom de l'élément : *NF_F_FW_EXT_EVENT*	Action sur le connecteur de Cisco Secure Firewall
2 (Flux supprimé)	> 2000 (indique le motif de fin)	Envoyer le flux à Cisco Secure Workload
3 (Flux refusé)	1001 (refusé par la liste de contrôle d'accès d'entrée)	Envoyer le flux avec le statut rejeté à Cisco Secure Workload
	1002 (refusé par la liste de contrôle d'accès de sortie)	
	1003 (connexion refusée par l'interface ASA ou ICMP(v6) refusé au périphérique)	
	1004 (le premier paquet sur TCP n'est pas SYN)	
4 (Alerte de flux)	Ce n'est pas important	Aucune opération
5 (Flux mis à jour)	Ce n'est pas important	Envoyer le flux à Cisco Secure Workload

Basé sur l'enregistrement NSEL, le connecteur de Cisco Secure Firewall envoie l'observation de flux à Cisco Secure Workload. Les enregistrements de flux de la NSEL sont bidirectionnels. Ainsi, le connecteur Cisco Secure Firewall envoie deux flux : le flux aller et le flux inverse vers Cisco Secure Workload.

Voici les détails sur l'observation de flux envoyées par le connecteur de Cisco Secure Firewall à Cisco Secure Workload.

Observation du flux aller

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Source Port (port source)	7	*NF_F_SRC_PORT*
Adresse de destination	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Destination Port (port de destination)	11	*NF_F_DST_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	231	*NF_F_FWD_FLOW_DELTA_BYTES*

Champ	ID d'élément NSEL	Nom d'élément NSEL
Nombre de paquets	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Information de flux inverse

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Source Port (port source)	11	*NF_F_DST_PORT*
Adresse de destination	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Destination Port (port de destination)	7	*NF_F_SRC_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	232	*NF_F_REV_FLOW_DELTA_BYTES*
Nombre de paquets	299	*NF_F_REV_FLOW_DELTA_PACKETS*

NAT

Si le flux client vers ASA est avec NAT, les enregistrements de flux NSEL indiquent l'adresse IP/le port avec NAT du côté serveur. Le connecteur de Cisco Secure Firewall utilise ces informations pour relier les flux du serveur à l'ASA et de l'ASA au client.

Voici l'enregistrement de flux avec NAT vers l'avant.

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Source Port (port source)	227	*NF_F_XLATE_SRC_PORT*
Adresse de destination	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Destination Port (port de destination)	228	*NF_F_XLATE_DST_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*

Champ	ID d'élément NSEL	Nom d'élément NSEL
Nombre d'octets	231	*NF_F_FWD_FLOW_DELTA_BYTES*
Nombre de paquets	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Le flux aller sera marqué comme étant lié à l'enregistrement de flux avec NAT dans la direction aller (et vice versa).

Voici l'enregistrement de flux avec NAT dans le sens inverse

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Source Port (port source)	228	*NF_F_XLATE_DST_PORT*
Adresse de destination	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Destination Port (port de destination)	227	*NF_F_XLATE_SRC_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	232	*NF_F_REV_FLOW_DELTA_BYTES*
Nombre de paquets	299	*NF_F_REV_FLOW_DELTA_PACKETS*

Le flux inverse sera marqué comme étant lié à l'enregistrement du flux avec NAT dans la direction inverse (et vice versa).

Note Seuls les ID d'élément NSEL répertoriés dans cette section sont pris en charge par le connecteur Cisco Secure Firewall.

Heuristique des indicateurs TCP

Les enregistrements NSEL ne contiennent pas d'information sur les indicateurs TCP. Le connecteur Cisco Secure Firewall utilise la méthode heuristique suivante pour définir les indicateurs TCP afin que les flux puissent être analysés de manière plus approfondie par la recherche automatique de politiques :

- S'il y a au moins un paquet de transfert, ajoute `SYN` aux indicateurs TCP de flux aller.
- S'il y a au moins deux paquets aller et un paquet retour, ajoute `ACK` aux indicateurs TCP de flux aller et `SYN-ACK` aux indicateurs TCP de flux inverse.
- Si la condition précédente est vérifiée et que l'événement de flux est Flux supprimé, ajoute `FIN` aux indicateurs TCP aller et arrière.

How to Configure NSEL on Secure Firewall ASA

The following steps are guidelines on how to configure NSEL and export NetFlow packets to a collector (i.e., Secure Firewall connector). Please also refer to the official Cisco configuration guide at Cisco Secure Firewall ASA NetFlow Implementation Guide for more details.

Here is an example NSEL configuration.

```
flow-export destination outside 172.29.142.27 4729
flow-export template timeout-rate 1
!
policy-map flow_export_policy
  class class-default
  flow-export event-type flow-create destination 172.29.142.27
  flow-export event-type flow-teardown destination 172.29.142.27
  flow-export event-type flow-denied destination 172.29.142.27
  flow-export event-type flow-update destination 172.29.142.27
  user-statistics accounting
service-policy flow_export_policy global
```

In this example, Secure Firewall ASA appliance is configured to sent NetFlow packets to *172.29.142.27* on port *4729*. In addition, *flow-export* actions are enabled on *flow-create*, *flow-teardown*, *flow-denied*, and *flow-update* events. When these flow events occur on ASA, a NetFlow record is generated and sent to the destination specified in the configuration.

Assuming a Secure Firewall connector is enabled on Cisco Secure Workload and listening on *172.29.142.27:4729* in a Cisco Secure Workload Ingest appliance, the connector will receive NetFlow packets from Secure Firewall ASA appliance. The connector processes the NetFlow records as discussed in Gestion des événements NSELand exports flow observations to Secure Workload. In addition, for NATed flows, the connector stitches the related flows (client-side and server-side) flows.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

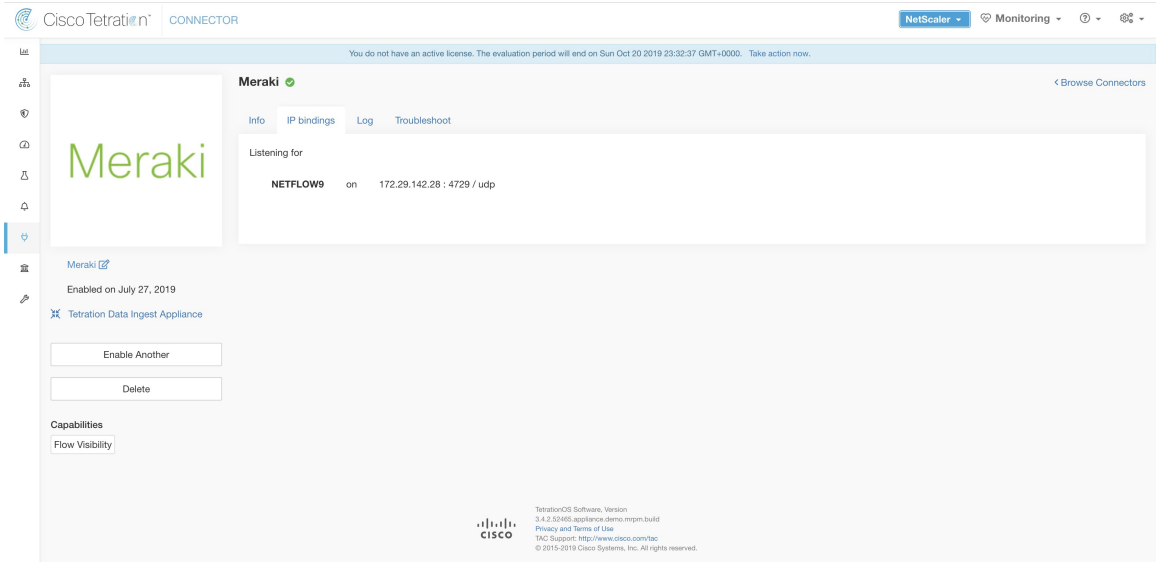
Unité	Limite
Nombre maximal de connecteurs Cisco Secure Firewall sur un dispositif d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs Cisco Secure Firewall sur un détenteur (portée racine)	10

Unité	Limite
Nombre maximal de connecteurs Cisco Secure Firewall sur Cisco Secure Workload	100

Connecteur Meraki

Le connecteur Meraki permet à Cisco Secure Workload d'acquérir les observations de flux des pare-feu Meraki (inclus dans les appareils de sécurité et les points d'accès sans fil Meraki MX). Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les commutateurs Cisco relayent les enregistrements NetFlow au connecteur Meraki hébergé dans un appareil d'acquisition Cisco Secure Workload pour le traitement.

Figure 66: Connecteur Meraki



Qu'est-ce que NetFlow

Le protocole NetFlow permet aux périphériques réseau comme le pare-feu Meraki d'agréger le trafic qui les traverse en flux et d'exporter ces flux vers un collecteur de flux. Le collecteur de flux reçoit ces enregistrements de flux et les stocke pour les interroger et les analyser hors ligne.

En règle générale, la configuration comprend les étapes suivantes :

1. Activer les rapports statistiques NetFlow sur le pare-feu Meraki.
2. Configurez les informations de point terminal du collecteur NetFlow sur le pare-feu Meraki.

Acquisition de flux dans Cisco Secure Workload

Le connecteur Meraki est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements de flux des pare-feu Meraki configurés pour exporter les statistiques de trafic NetFlow. Il traite les enregistrements NetFlow et envoie les observations de flux signalées par les pare-feu Meraki à Cisco Secure Workload pour une analyse de flux. Un connecteur Meraki peut être activé sur un appareil d'acquisition Cisco Secure Workload et s'exécute en tant que conteneur Docker.

Le connecteur Meraki s'enregistre également auprès de Cisco Secure Workload en tant qu'agent Meraki Cisco Secure Workload. Le connecteur Meraki désencapsule les paquets de protocole NetFlow (c.-à-d. les enregistrements de flux); traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Note Le connecteur Meraki prend en charge le protocole NetFlow v9.

Note Chaque connecteur Meraki ne doit signaler les flux que pour un VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Gestion des enregistrements NetFlow

Selon l'enregistrement NetFlow, le connecteur Meraki envoie l'observation de flux à Cisco Secure Workload. Les enregistrements de flux Meraki NetFlow sont bidirectionnels. Ainsi, le connecteur Meraki envoie deux flux : le flux aller et le flux inverse à Cisco Secure Workload.

Voici les détails sur l'observation de flux envoyée par le connecteur Meraki à Cisco Secure Workload.

Observation du flux aller

Champ	ID d'élément	Nom de l'élément
Protocole	4	*protocolIdentifier*
Adresse de la source	8	*sourceIPv4Address*
Source Port (port source)	7	*sourceTransportPort*
Adresse de destination	12	*destinationIPv4Address*
Destination Port (port de destination)	11	*destinationTransportPort*
Nombre d'octets	1	*octetDeltaCount*
Nombre de paquets	2	*packetDeltaCount*
Heure de début du flux		Défini en fonction du moment de la réception de l'enregistrement NetFlow pour ce flux sur le connecteur

Information de flux inverse

Champ	ID d'élément	
Protocole	4	*protocolIdentifier*
Adresse de la source	8	*sourceIPv4Address*
Source Port (port source)	7	*sourceTransportPort*
Adresse de destination	12	*destinationIPv4Address*
Destination Port (port de destination)	11	*destinationTransportPort*
Nombre d'octets	23	*postOctetDeltaCount*
Nombre de paquets	24	*postPacketDeltaCount*
Heure de début du flux		Défini en fonction du moment de la réception de l'enregistrement NetFlow pour ce flux sur le connecteur

Comment configurer NetFlow sur un pare-feu Meraki

Les étapes suivantes montrent comment configurer les rapports NetFlow sur le pare-feu Meraki.

Procedure

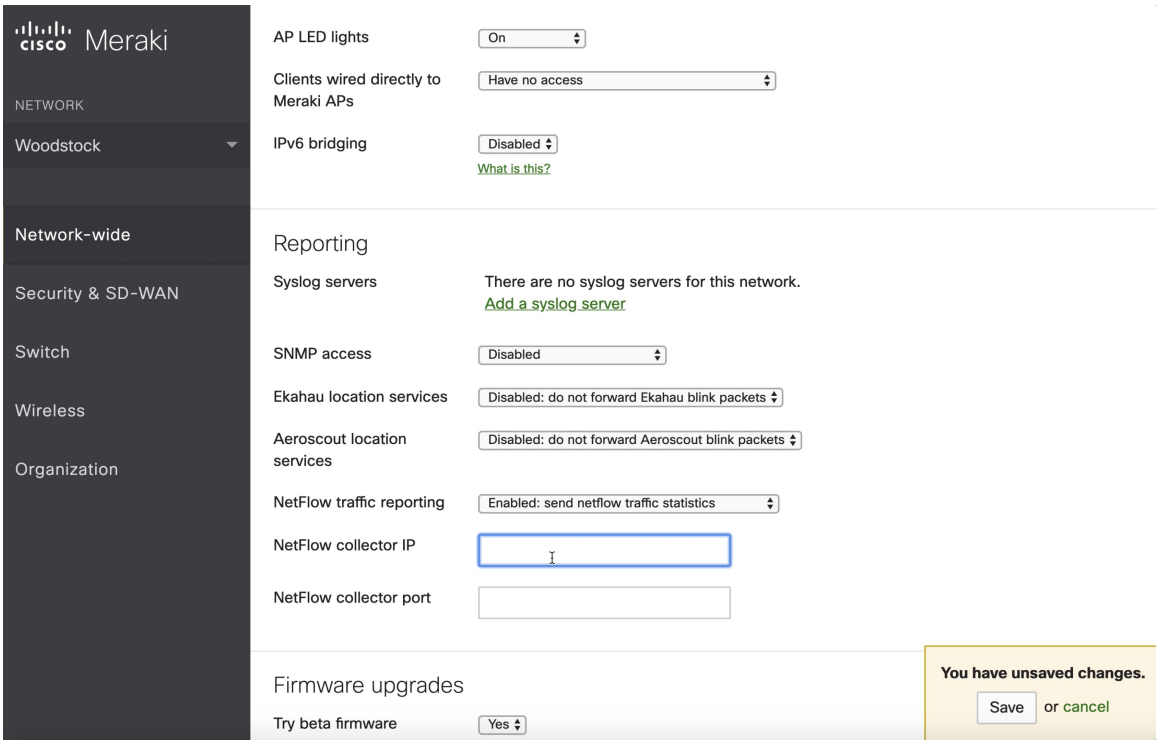
Étape 1 Connectez-vous à la console de l'interface utilisateur Meraki.

Étape 2 Naviguez jusqu'à **Network-wide (À l'échelle du réseau)** > **General (Général)**. Dans les paramètres de *rapport*, activez **les rapports sur le trafic NetFlow** et assurez-vous que la valeur est définie sur *Activé : envoyer les statistiques de trafic NetFlow.*

Étape 3 Réglez **NetFlow collector IP** (adresse IP du collecteur NetFlow) et **NetFlow collector port** (port du collecteur NetFlow) sur l'adresse IP et le port sur lesquels le connecteur Meraki écoute dans le dispositif d'acquisition Cisco Secure Workload. Le port par défaut sur lequel le connecteur Meraki écoute les enregistrements NetFlow est 4729.

Étape 4 Enregistrer les modifications

Figure 67: Activation de NetFlow sur un pare-feu Meraki



Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

En outre, les ports d'écoute du protocole NetFlow v9 sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs Meraki sur un dispositif d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs Meraki sur un détenteur (portée racine)	10

Unité	Limite
Nombre maximal de connecteurs Meraki sur Cisco Secure Workload	100

Connecteur ERSPAN

Le connecteur ERSPAN permet à Cisco Secure Workload d'acquérir les observations de flux des routeurs et des commutateurs du réseau. Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter d'agents logiciels, car les commutateurs Cisco relayent le trafic des hôtes vers le connecteur ERSPAN pour traitement.

Qu'est-ce qu'ERSPAN?

L'analyseur ERSPAN (Encapsulating Remote Switch Port Analyzer) est une fonctionnalité présente dans la plupart des commutateurs Cisco. Il reproduit les trames vues par un périphérique réseau, les encapsule dans un paquet IP et les envoie à un analyseur distant. Les utilisateurs peuvent sélectionner une liste d'interfaces ou de VLAN sur le commutateur à surveiller.

En général, l'installation consiste à configurer la ou les sessions de surveillance ERSPAN de source sur un ou plusieurs périphériques de réseau et à configurer la ou les sessions de surveillance ERSPAN de destination sur le ou les périphériques de réseau distants directement connectés à un analyseur de trafic.

Le connecteur ERSPAN Cisco Secure Workload fournit à la fois la session ERSPAN de destination et les fonctionnalités d'analyse du trafic; il n'est donc pas nécessaire de configurer des sessions de destination sur les commutateurs dotés de la solution Cisco Secure Workload.

Que sont les agents SPAN

Chaque connecteur ERSPAN enregistre un agent SPAN auprès de la grappe. Les agents SPAN Cisco Secure Workload sont des agents Cisco Secure Workload standard configurés pour traiter uniquement les paquets ERSPAN : à l'instar des sessions ERSPAN de destination de Cisco, ils désencapsulent les trames en miroir; ils traitent ensuite les flux et en rendent compte comme un agent Cisco Secure Workload normal. Contrairement aux agents de visibilité approfondie, ils ne signalent aucune information sur les processus ou l'interface.

Qu'est-ce que l'appareil d'acquisition pour ERSPAN

L'appareil d'acquisition Cisco Secure Workload pour ERSPAN est une machine virtuelle qui fait fonctionner en interne trois connecteurs ERSPAN Cisco Secure Workload. Il utilise le même OVA ou QCOW2 que l'appareil d'acquisition classique.

Chaque connecteur s'exécute dans un conteneur Docker dédié auquel une vNIC et deux cœurs vCPU sans quota de limite sont exclusivement affectés.

Le connecteur ERSPAN enregistre un agent SPAN avec la grappe avec le nom d'hôte du conteneur :<Nom d'hôte de la machine virtuelle> -<Adresse IP de l'interface>.

Les connecteurs et les agents sont conservés ou restaurés lors du blocage ou du redémarrage de la machine virtuelle, du daemon ou du conteneur Docker.

Remarque L'état du connecteur ERSPAN est renvoyé à la page Connector (connecteur). Consultez la page Agent List (Liste des agents) et vérifiez l'état des agents SPAN correspondants.

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs. Pour les connecteurs ERSPAN, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Comment configurer la session ERSPAN source

Les étapes suivantes concernent un commutateur Nexus 9000. Les configurations peuvent différer légèrement pour les autres plateformes Cisco. Pour la configuration d'une plateforme Cisco, consultez le Guide de l'utilisateur du Cisco Secure Workload.

Illustration 68 : Configurer la source ERSPAN sur Cisco Nexus 9000

```
Enter the configuration mode
# config terminal

Configure the erspan source IP address
(config)# monitor erspan origin ip-address 172.28.126.1 global

Create and configure the source erspan session
(config)# monitor session 10 type erspan-source
(config-erspan-src)# source interface ethernet 1/23 both
(config-erspan-src)# source vlan 315, 512
(config-erspan-src)# destination ip 172.28.126.194

Turn on the monitor session
(config-erspan-src)# no shut

Persist the configuration
# copy runnin-config startup-config
```

Les étapes ci-dessus ont créé une session ERSPAN source avec l'ID 10. Le commutateur mettra en miroir les trames entrant et sortant (à la fois) de l'interface eth1/23 et de celles sur les VLANS 315 et 512. Le paquet GRE externe transportant la trame miroir aura l'IP source 172.28.126.1 (doit être l'adresse d'une interface L3 sur ce commutateur) et l'IP de destination 172.28.126.194. Il s'agit de l'une des adresses IP configurées sur la machine virtuelle ERSPAN.

Formats ERSPAN pris en charge

Les agents SPAN Cisco Secure Workload peuvent traiter les paquets ERSPAN de type I, II et II décrits dans la RFC ERSPANproposée. Par conséquent, ils peuvent traiter les paquets ERSPAN générés par les périphériques Cisco. Parmi les formats non conformes à la RFC, ils peuvent traiter les paquets ERSPAN générés par VMware vSphere Distributed Switch (VDS).

Considérations relatives aux performances lors de la configuration de la source ERSPAN

Choisissez avec soin la liste de ports/VLAN de la source ERSPAN. Bien que l'agent SPAN dispose de deux vCPU dédiés, la session peut générer une quantité considérable de paquets, ce qui pourrait saturer la puissance de traitement de l'agent. Si un agent reçoit plus de paquets qu'il ne peut en traiter, cela sera indiqué dans le graphique Paquets manquants de l'agent sur la page Deep Visibility Agent (Agent de visibilité approfondie) de la grappe.

Un réglage plus fin des trames sur lesquelles la source ERSPAN sera mise en miroir peut être obtenu à l'aide de politiques ACL, généralement à l'aide du mot-clé de configuration filter.

Si le commutateur le prend en charge, la session source ERSPAN peut être configurée pour modifier l'unité de transport maximale (MTU) du paquet ERSPAN (généralement la valeur par défaut de 1500 octets), généralement au moyen d'un mot-clé mtu. La diminuer limitera l'utilisation de la bande passante ERSPAN dans votre infrastructure réseau, mais n'aura aucun effet sur la charge de l'agent SPAN, étant donné que la charge de travail de l'agent est par paquet. Lorsque vous réduisez cette valeur, prévoyez de la place pour 160 octets pour la trame miroir. Pour plus de détails sur le surdébit d'en-tête ERSPAN, consultez la demande d'informations sur ERSPAN RFCproposée.

Il existe trois versions d'ERSPAN. Plus la version est petite, plus le surdébit de l'en-tête ERSPAN est faible. Les versions II et III permettent d'appliquer des politiques de qualité de service (QoS) aux paquets ERSPAN et fournissent des renseignements sur le VLAN. La version III comporte encore plus de paramètres. La version II est généralement celle par défaut des commutateurs Cisco. Bien que les agents ERSPAN Cisco Secure Workload prennent en charge les trois versions, pour le moment ils n'utilisent aucune information supplémentaire que transportent les paquets ERSPAN versions II et III.

Questions de sécurité.

Le système d'exploitation invité de la machine virtuelle d'acquisition pour ERSPAN est CentOS 7.9, dont les paquets serveur/clients OpenSSL ont été supprimés.

Remarque CentOS 7.9 est le système d'exploitation invité pour les appareils virtuels d'acquisition et de périphérie de Cisco Secure Workload 3.8.1.19 et les versions antérieures. À partir de la version 3.8.1.36 de Cisco Secure Workload, le système d'exploitation est AlmaLinux 9.2.

Une fois que la machine virtuelle est démarrée et que les conteneurs d'agents SPAN sont déployés (l'opération prend quelques minutes lors du premier démarrage uniquement), aucune interface réseau, hormis la boucle avec retour, ne sera présente dans la machine virtuelle. Par conséquent, la seule façon d'accéder à l'appareil est via sa console.

L'interface réseau de la machine virtuelle est maintenant déplacée à l'intérieur des conteneurs Docker. Les conteneurs exécutent une image Docker basée sur centos : 7.9.2009 sans port TCP/UDP ouvert.

Remarque À partir de la version 3.8.1.36 de Cisco Secure Workload, les conteneurs exécutent almalinux/9-base:9.2.

En outre, les conteneurs sont exécutés avec les privilèges de base (option no –privileged) plus la capacité NET_ADMIN.

Dans le cas improbable où un conteneur serait contaminé, le système d'exploitation invité de la machine virtuelle ne devrait pas pouvoir être contaminé depuis l'intérieur du conteneur.

Toutes les autres considérations de sécurité valides pour les agents Cisco Secure Workload exécutés dans un hôte s'appliquent également aux agents SPAN Cisco Secure Workload exécutés dans les conteneurs Docker.

Dépannage

Une fois que les agents SPAN sont à l'état actif dans la page Monitoring/Agent Overview (Surveillance/Aperçu de l'agent) de la grappe, aucune action n'est nécessaire sur la machine virtuelle ERSPAN et l'utilisateur n'a pas besoin de s'y connecter. Si cela ne se produit pas ou si les flux ne sont pas signalés à la grappe, les renseignements suivants permettront d'identifier les problèmes de déploiement.

Dans des conditions normales, sur la machine virtuelle :

- `systemctl status tet_vm_setup` signale un service *inactif* avec l'état de sortie *SUCCESS*;
- `systemctl status tet-nic-driver` signale un service *actif*;
- `docker network ls` signale cinq réseaux : `host, none` et trois `erspan-<iface name>;`
- `ip link` signale uniquement l'interface de boucle avec retour;
- `docker ps` signale trois conteneurs en cours d'exécution;
- `docker logs <cid>` pour chaque conteneur, contient le message :`NFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)` (Succès du NFO : le capteur tet est entré dans l'état RUNNING, le processus est resté en place pendant > 1 seconde (startsecs).
- `docker exec <cid> ifconfig` ne signale qu'une seule interface, en plus de la boucle avec retour;
- `docker exec <cid> route -n` signale la passerelle par défaut;
- `docker exec <cid> iptables -t raw -S PREROUTING` signale la règle `-A PREROUTING-p gre -j DROP;`

Si l'un des éléments ci-dessus n'est pas vérifié, vérifiez les journaux du script de déploiement dans `/local/tetration/logs/tet_vm_setup.log` pour connaître la raison de l'échec du déploiement des conteneurs d'agents SPAN.

Tout autre problème d'enregistrement ou de connectivité des agents peut être résolu de la même manière que pour les agents exécutés sur un hôte, à l'aide de la commande *docker exec* :

- `docker exec <cid> ps -ef` signale les deux instances `tet-engine, tet-engine check_conf` et deux instances `/usr/local/tet/tet-sensor -f /usr/local/tet/conf/.sensor_config`, une avec l'utilisateur racine et une avec l'utilisateur tet -sensor, ainsi que l'instance gestionnaire de processus `/usr/bin/ python /usr/bin/supervisord -c /etc/supervisord.conf -n`.
- `docker exec <cid> cat /usr/local/tet/log/tet-sensor.log` affiche les journaux de l'agent;
- `docker exec <cid> cat /usr/local/tet/log/fetch_sensor_id.log` affiche les journaux des enregistrements de l'agent;
- `docker exec <cid> cat /usr/local/tet/log/check_conf_update.log` affiche les journaux d'interrogation de la mise à jour de la configuration;

  Si nécessaire, le trafic vers/depuis le conteneur peut être surveillé à l'aide de la commande tcpdump après avoir été défini dans l'espace de nom réseau du conteneur :

  1. Récupérez l'espace de noms réseau du conteneur (SandboxKey) à l'aide de docker inspect <cid> | grep SandboxKey;
  2. Inscrit dans l'espace de noms du réseau du conteneur nsenter --net=/var/run/docker/netns/...;
  3. Surveillez le trafic tcpdump -i eth0 -n.

Limites

Unité	Limite
Nombre maximal de connecteurs ERSPAN sur un appareil d'acquisition (ingest appliance) Cisco Secure Workload	3

Unité	Limite
Nombre maximal de connecteurs ERSPAN sur un détenteur (portée racine)	24 (12 pour TaaS)
Nombre maximal de connecteurs ERSPAN sur Cisco Secure Workload	450

Connecteurs pour points terminaux

Les connecteurs pour points terminaux fournissent un contexte de point terminal pour Cisco Secure Workload.

Connecteur	Description	Déployé sur une appliance virtuelle
AnyConnect	Recueillez des données de télémétrie à partir du module de visibilité réseau (Network Visibility Module ou NVM) Cisco AnyConnect et enrichissez les inventaires de points terminaux avec les attributs des utilisateurs.	Acquisition de Cisco Secure Workload
ISE	Recueillez des renseignements sur les points terminaux et les inventaires gérés par les appareils Cisco ISE et enrichissez les inventaires des points terminaux avec des attributs utilisateur et des étiquettes de groupe sécurisées (SGL).	Cisco Secure Workload Edge

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

AnyConnect Connector

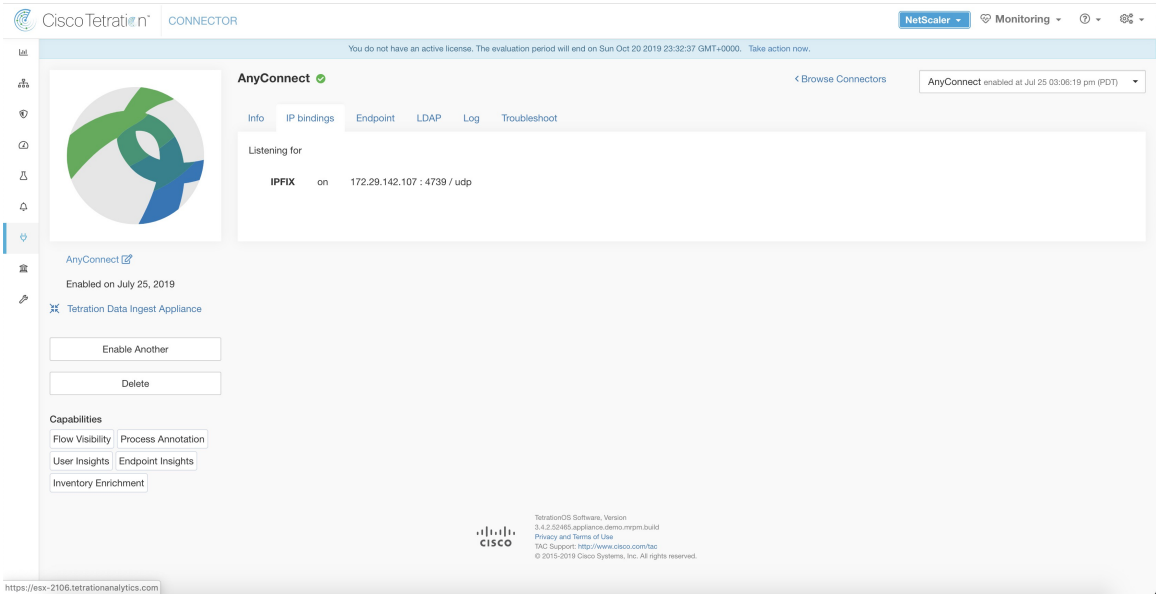
AnyConnect connector monitors endpoints that run Cisco AnyConnect Secure Mobility Client with Network Visibility Module (NVM). Using this solution, the hosts do not need to run any software agents on endpoints, because NVM sends host, interface, and flow records in IPFIX format to a collector (e.g., AnyConnect connector).

AnyConnect connector does the following high-level functions.

1. Register each endpoint (supported user devices such as a desktop, a laptop, or a smartphone) on Cisco Cisco Secure Workload as an AnyConnect agent.
2. Update interface snapshots from these endpoints with Secure Workload.
3. Send flow information exported by these endpoints to Cisco Secure Workload collectors.
4. Periodically send process snapshots for processes that generate flows on the endpoints tracked by the AnyConnect connector.

5. Label endpoint interface IP addresses with Lightweight Directory Access Protocol (LDAP) attributes corresponding to the logged-in-user at each endpoint.

Figure 69: AnyConnect connector



Qu'est-ce qu'AnyConnect NVM?

AnyConnect NVM offre une visibilité et une surveillance du comportement des terminaux et des utilisateurs sur site et hors site. Il recueille des informations à partir des points terminaux qui incluent le contexte suivant.

1. **Contexte d'appareil/point terminal** : informations spécifiques à l'appareil ou au point terminal.
2. **Contexte utilisateur** : utilisateurs associés au flux.
3. **Contexte d'application** : processus associés au flux.
4. **Contexte de l'emplacement** : attributs propres à l'emplacement, si disponibles.
5. **Contexte de destination** : nom de domaine complet (FQDN) de la destination. AnyConnect NVM génère trois types d'enregistrements.

Enregistrement NVM	Description
Enregistrement de point terminal	Informations sur le périphérique ou le point terminal, y compris l'identifiant unique de périphérique (UDID), le nom d'hôte, le nom du système d'exploitation, la version du système d'exploitation et le fabricant.
Enregistrement d'interface	Informations sur chaque interface du point terminal, y compris l'UDID du point terminal, l'identifiant unique de l'interface (UID), l'indice d'interface, le type d'interface, le nom de l'interface et l'adresse MAC.

Enregistrement NVM	Description
Enregistrement de flux	Renseignements sur les flux observés sur le point terminal, y compris l'UDID du point terminal, l'UID de l'interface, le 5-tuple (source/destination ip/port et protocole), le nombre d'octets entrants/sortants, les renseignements sur le processus, les renseignements sur l'utilisateur et le nom de domaine complet de la destination.

Chaque enregistrement est généré et exporté au format de protocole IPFIX. Lorsque le périphérique se trouve dans un réseau de confiance (sur site/VPN), AnyConnect NVM exporte les enregistrements vers un collecteur configuré. Le connecteur AnyConnect est un exemple de collecteur IPFIX qui peut recevoir et traiter le flux IPFIX de AnyConnect NVM.

Note Le connecteur AnyConnect prend en charge AnyConnect NVM à partir des versions 4.2 et ultérieures de Cisco AnyConnect Secure Mobility Client.

How to configure AnyConnect NVM

See How to Implement AnyConnect NVM document for step by step instructions on how to implement AnyConnect NVM using either Cisco Secure Firewall ASA or Cisco Identity Services engine (ISE). Once NVM module is deployed, an NVM profile should be specified and pushed to and installed on the endpoints running Cisco AnyConnect Secure Mobility Client. When specifying NVM profile, the IPFIX collector should be configured to point to AnyConnect connector on port 4739.

AnyConnect connector also registers with Cisco Secure Workload as a Cisco Secure Workload AnyConnect Proxy agent.

Traitement des enregistrements NVM

Le connecteur AnyConnect traite les enregistrements NVM AnyConnect comme indiqué ci-dessous.

Enregistrement de point terminal

Lors de la réception d'un enregistrement de point terminal, le connecteur AnyConnect enregistre ce point terminal en tant qu'agent AnyConnect sur la charge de travail sécurisée. Le connecteur AnyConnect utilise les renseignements spécifiques au point terminal présents dans l'enregistrement NVM avec le certificat du connecteur AnyConnect pour enregistrer le point terminal. Une fois qu'un point terminal est enregistré, le plan de données du point terminal est activé en créant une nouvelle connexion à l'un des collecteurs dans Cisco Secure Workload. En fonction de l'activité (enregistrements de flux) de ce point terminal, le connecteur AnyConnect connecte l'agent AnyConnect correspondant à ce point à la grappe périodiquement (20 à 30 minutes).

AnyConnect NVM commence à diffuser la version de l'agent à partir de la version 4.9. Par défaut, le point terminal AnyConnect est enregistré en tant que version 4.2.x sur Cisco Secure Workload. Cette version indique la version minimale NVM AnyConnect prise en charge. Pour les points terminaux AnyConnect dotés dans la version 4.9 ou ultérieure, l'agent AnyConnect correspondant sur Cisco Secure Workload affichera la version réelle installée.

Note La version installée de l'agent AnyConnect n'est pas contrôlée par Cisco Secure Workload. La tentative de mise à niveau de l'agent terminal AnyConnect sur l'interface utilisateur Cisco Secure Workload n'a pas d'effet.

Enregistrement d'interface

L'adresse IP de l'enregistrement d'interface pour une interface donnée ne fait pas partie de l'enregistrement d'interface NVM AnyConnect. L'adresse IP d'une interface est déterminée lorsque les enregistrements de flux commencent à être envoyés à partir du point terminal pour cette interface. Une fois que l'adresse IP est déterminée pour une interface, le connecteur AnyConnect envoie un instantané complet de toutes les interfaces de ce point terminal dont l'adresse IP est déterminée au serveur de configuration de Cisco Secure Workload. Le VRF est ainsi associé aux données de l'interface et les flux arrivant sur ces interfaces seront désormais marqués par ce VRF.

Enregistrement de flux

Lors de la réception d'un enregistrement de flux, le connecteur AnyConnect le traduit au format que Cisco Secure Workload comprend et envoie FlowInfo sur le plan de données correspondant à ce point terminal. En outre, il stocke localement les informations de processus incluses dans l'enregistrement de flux. De plus, si une configuration LDAP est fournie au connecteur AnyConnect, celui-ci détermine les valeurs des attributs LDAP configurés de l'utilisateur connecté du point terminal. Les attributs sont associés à l'adresse IP du point terminal où le flux s'est produit. Périodiquement, les informations sur les processus et les étiquettes des utilisateurs sont transmises à Cisco Secure Workload.

Note Chaque connecteur AnyConnect ne signalera que les points terminaux, les interfaces et les flux pour un VRF. Les points terminaux et les interfaces signalés par le connecteur AnyConnect sont associés au VRF en fonction de la configuration du VRF de l'agent dans Cisco Secure Workload. Les flux exportés par l'agent de connecteur AnyConnect au nom du point terminal AnyConnect appartiennent au même VRF. Pour configurer le VRF pour l'agent, accédez à : **Manage (Gestion)** > **Agents (Agents)** puis cliquez sur l'onglet **Configuration**. Dans cette page, dans la section « Agent Remote VRF Configurations » (configurations de VRF à distance de l'agent), cliquez sur « Create Config » (Créer une configuration) et fournissez les détails du connecteur AnyConnect. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP de l'hôte sur lequel l'agent est installé, et la plage de numéros de ports qui peuvent potentiellement envoyer des enregistrements de flux à la grappe.

UDID en double dans les points terminaux Windows

Si des machines de point terminal sont clonées à partir de la même image d'or, il est possible que les UDID de tous les points terminaux clonés soient identiques. Dans ce cas, le connecteur AnyConnect reçoit les enregistrements de point terminal de ces points terminaux avec le même UDID et les enregistre sur Cisco Secure Workload avec le même UDID. Lorsque des enregistrements d'interface ou de flux sont reçus par le connecteur de ces points terminaux, le connecteur ne peut pas déterminer l'agent AnyConnect correct sur Cisco Secure Workload auquel associer les données. Le connecteur associe toutes les données à un seul point terminal (et il n'est pas déterministe).

Pour résoudre ce problème, la version 4.8 d'AnyConnect NVM est livrée avec un outil appelé *dartcli.exe* pour déterminer et régénérer l'UDID sur le point terminal.

- *dartcli.exe -u* récupère l'UDID du point terminal.
- *dartcli.exe -nu* régénère l'UDID du point terminal. Pour exécuter cet outil, procédez comme suit :

```
    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 8D0D1E8FA0AB09BE82599F10068593E41EF1BFFF

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-nu
    Are you sure you want to re-generate UDID [y/n]: y
    Adding nonce success
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5
```

Tâches périodiques

Périodiquement, le connecteur AnyConnect envoie des instantanés de processus et des étiquettes d'utilisateur sur les inventaires de points terminaux AnyConnect.

1. **Instantanés de processus** : toutes les 5 minutes, le connecteur AnyConnect parcoure les processus qu'il gère localement pendant cet intervalle et envoie un instantané de processus pour tous les points terminaux qui ont reçu des flux pendant cet intervalle.
2. **Étiquettes utilisateur** : toutes les 2 minutes, le connecteur AnyConnect parcourt les étiquettes utilisateur LDAP qu'il gère localement et met à jour les étiquettes utilisateur sur ces adresses IP.

Pour les étiquettes d'utilisateur, le connecteur AnyConnect crée un instantané local des attributs LDAP de tous les utilisateurs de l'organisation. Lorsque le connecteur AnyConnect est activé, la configuration LDAP (informations sur le serveur/port, attributs à récupérer pour un utilisateur, attribut qui contient le nom d'utilisateur) peut être fournie. De plus, les renseignements d'authentification de l'utilisateur LDAP pour accéder au serveur LDAP peuvent être fournis. Les renseignements d'authentification des utilisateurs LDAP sont chiffrés et ne sont jamais révélés dans le connecteur AnyConnect. Si vous le souhaitez, un certificat LDAP peut être fourni pour un accès sécurisé au serveur LDAP.

Note Le connecteur AnyConnect crée un nouvel instantané LDAP local toutes les 24 heures. Cet intervalle est configurable dans la configuration LDAP du connecteur.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *LDAP* : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour choisir l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Point terminal* : pour en savoir plus, consultez Configuration du point terminal.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs AnyConnect sur un appareil d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs AnyConnect sur un détenteur (portée racine)	50
Nombre maximal de connecteurs AnyConnect sur Cisco Secure Workload	500

ISE Connector

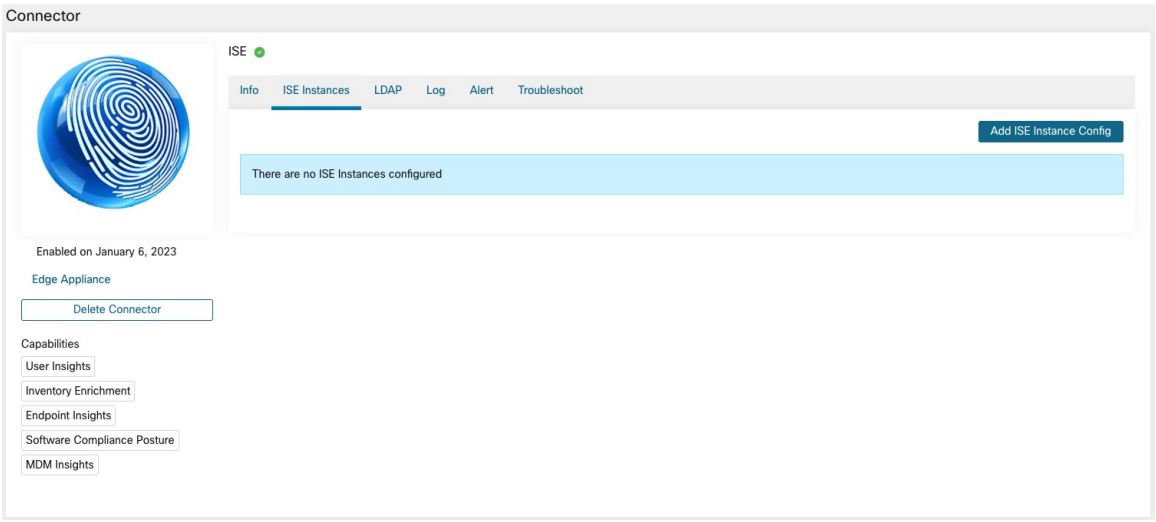
ISE connector in Secure Workload connects with Cisco Identity Services Engine (ISE), using Cisco Platform Exchange Grid (pxGrid), to retrieve contextual information about endpoints reported by ISE. Using these solutions, we can obtain enriched metadata for endpoints.

The ISE connector in Secure Workload connects with Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC) using the Cisco Platform Exchange Grid (pxGrid), to retrieve contextual information, such as metadata, for endpoints reported by ISE.

An ISE connector performs these functions:

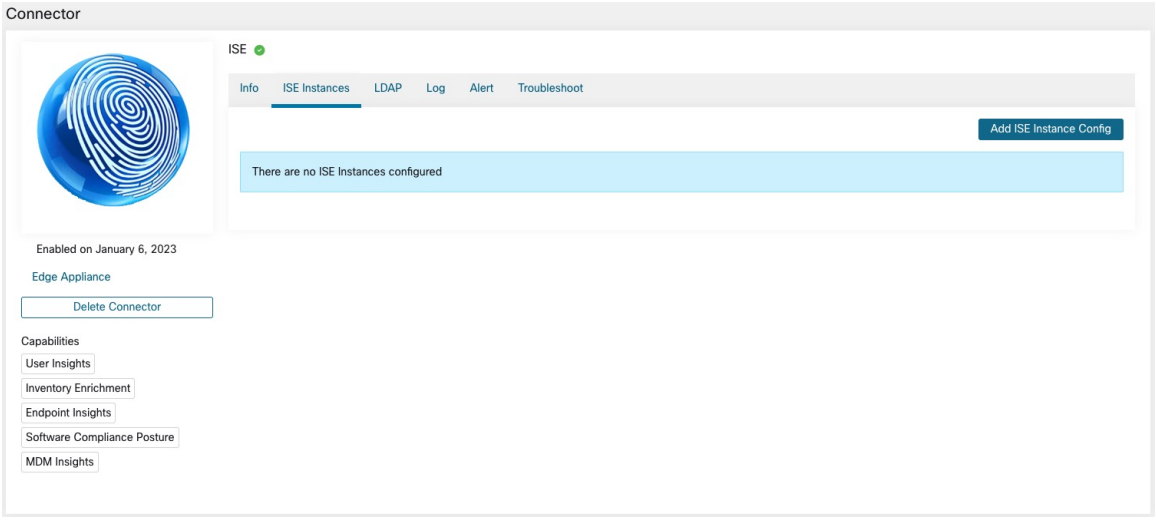
1. Register each endpoint viewed by ISE on Cisco Secure Workload as an ISE endpoint agent.
2. Update metadata information regarding these endpoints to Cisco Secure Workload including MDM details, authentication, Security Group labels, and others.
3. Periodically take a snapshot and update cluster with active endpoints visible on ISE.

Figure 70: ISE connector



1. Registers each endpoint that are identified as an ISE endpoint on Secure Workload.
2. Updates metadata information on Secure Workload regarding the endpoints, such as MDM details, authentication, Security Group labels, ISE group name, and ISE group type.
3. Periodically takes a snapshot and updates the cluster with active endpoints visible on the ISE.

Figure 71: ISE connector



Note Each ISE connector will register only endpoints and interfaces for one VRF. The endpoints and interfaces reported by ISE connector are associated with the VRF based on the Agent VRF configuration in Secure Workload. To configure the VRF for the agent, go to: **Manage** > **Agents** and click the **Configuration** tab. In this page, under the **Agent Remote VRF Configurations** section, click **Create Config** and provide the details about the ISE connector. The form requests the user to provide: the name of the VRF, IP subnet of the host on which the agent is installed, and range of port numbers that can potentially register ISE endpoints and interfaces on Secure Workload.

Note The ISE endpoint agents are not listed on the Agents List page; instead ISE endpoints with the attributes can be viewed on the Inventory page.

Comment configurer le connecteur

Note ISE version 2.4+ et ISE PIC version 3.1+ sont nécessaires pour cette intégration.

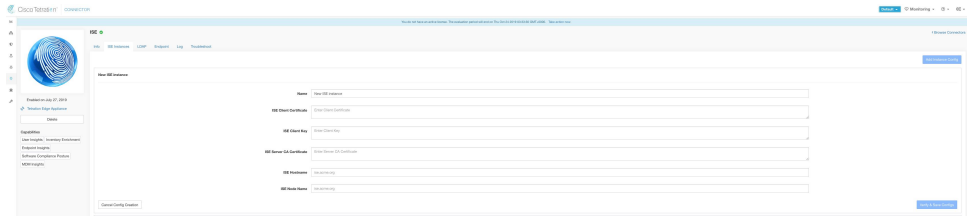
Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Pour les connecteurs ISE, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Les configurations suivantes sont autorisées sur le connecteur.

- *Instance ISE* : le connecteur ISE peut se connecter à plusieurs instances ISE en utilisant les configurations fournies. Chaque instance nécessite des renseignements d'authentification de certificat ISE ainsi qu'un nom d'hôte et un nom de nœud pour se connecter à ISE. Pour en savoir plus, consultez Configuration de l'instance ISE.
- *LDAP* : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour sélectionner l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Point terminal* : pour en savoir plus, consultez Configuration du point terminal.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration du point terminal.

Configuration de l'instance ISE

Figure 72: Configuration d'instance ISE



Note À partir de la version 3.7 de Cisco Secure Workload, le certificat SSL pour le nœud pxGrid de Cisco ISE nécessite d'autres noms de sujet (SAN) pour cette intégration. Assurez-vous que la configuration de certification des nœuds ISE est effectuée par votre administrateur ISE avant de procéder à l'intégration avec Cisco Secure Workload.

Pour vérifier le certificat de votre nœud pxGrid et confirmer si le SAN est configuré, vous devez procéder comme suit pour vérifier le certificat d'ISE.

Procedure

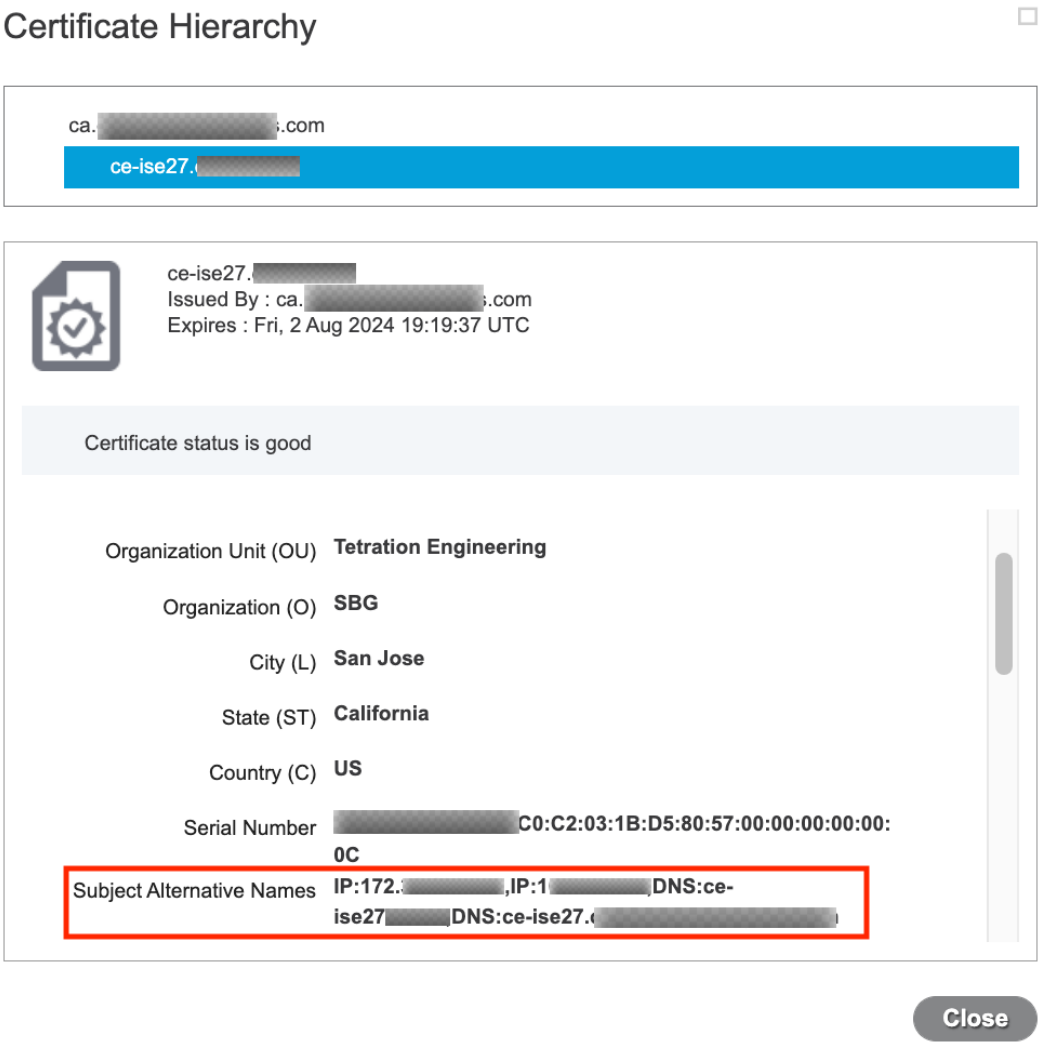
Étape 1 Rendez-vous à **Certificates** (Certificats) sous **Administration** > **System** (Système).

Étape 2 Sous **Certificate Management** (Gestion du certificat) , sélectionnez **System Certificates** (Certificat système), sélectionnez votre certificat pxGrid « utilisé par » et choisissez **View** (afficher) pour examiner le certificat de nœud pxGrid.

Étape 3 Faites défiler le certificat et vérifiez que les Subject Alternative Names (autres noms de sujet) sont configurés pour ce certificat.

Étape 4 Ce certificat doit être signé par une autorité de certification (CA) valide, qui doit également être utilisée pour signer le certificat client pxGrid utilisé par le connecteur Cisco Secure Workload ISE.

Figure 73: Exemple de certificat de nœud ISE valide



Étape 5 Vous pouvez maintenant générer la demande de signature de certificat client pxGrid en utilisant le modèle suivant sur n'importe quel hôte installé avec OpenSSL.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = YOUR_COUNTRY
ST = YOUR_STATE
L = YOUR_CITY
O = YOUR_ORGANIZATION
OU = YOUR_ORGANIZATION_UNIT
CN = ise-connector.example.com
[v3_req]
subjectKeyIdentifier = hash
```

```
basicConstraints = critical,CA:false
subjectAltName = @alt_names
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = serverAuth,clientAuth
[alt_names]
IP.1 = 10.x.x.x
DNS.1 = ise-connector.example.com
```

Enregistrez le fichier sous le nom « example-connector.cfg » et utilisez la commande OpenSSL de votre hôte pour générer une requête de signature de certificat (CSR) et la clé privée du certificat à l'aide de la commande suivante.

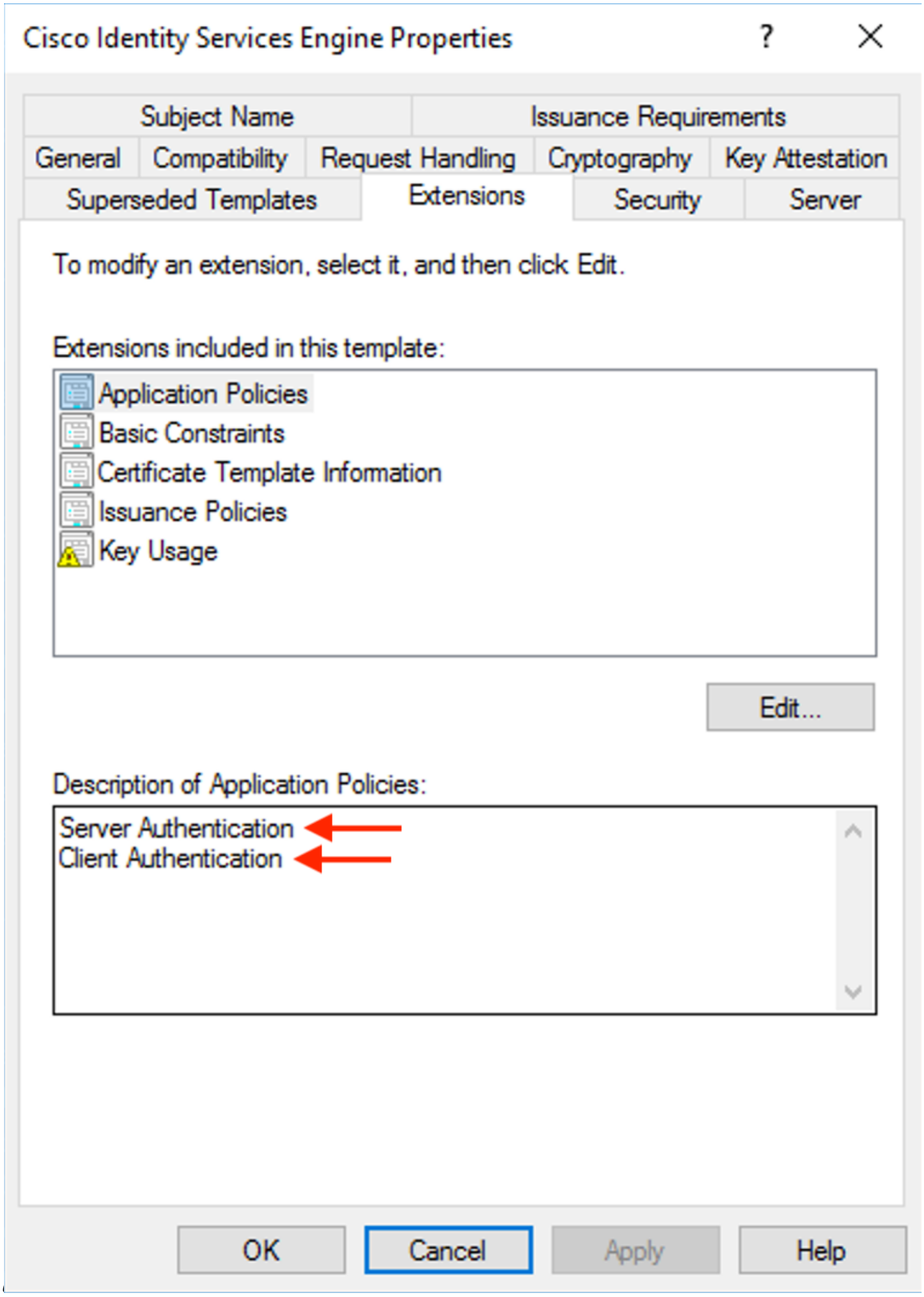
```
openssl req -newkey rsa:2048 -keyout example-connector.key -nodes -out example-connector.csr
 -config example-connector.cfg
```

Étape 6 Signez la requête de signature de certificat (CSR) de votre autorité de certification en utilisant un serveur d'autorité de certification Windows. Si vous utilisez également un serveur d'autorité de certification Windows, exécutez la commande suivante pour signer la CSR du client pxGrid.

```
certreq -submit -binary -attrib "CertificateTemplate:CiscoIdentityServicesEngine"
example-connector.csr example-connector.cer
```

Note L'autorité de certification Windows nécessite un modèle de certificat. Ce modèle doit contenir les extensions suivantes.

Figure 74: Extensions des politiques d'application pour un modèle de



Étape 7 Copiez le certificat client signé et l'autorité de certification racine au format PEM sur votre hôte. Il s'agit du même hôte qui génère la demande de signature de certificat (CSR) du client et la clé privée. Utilisez OpenSSL pour vous assurer que le certificat client est au format PEM X.509. Exécutez la commande suivante à l'aide d'OpenSSL pour convertir le certificat client signé au format PEM X.509.

```
openssl x509 -inform der -in example-connector.cer -out example-connector.pem
```

Étape 8 Vous pouvez également confirmer le PEM signé par l'autorité de certification en utilisant la commande suivante.

```
openssl verify -CAfile root-ca.example.com.pem example-connector.pem
example-connector.pem: OK
```

Note Pour le déploiement à nœuds multiples d'ISE avec pxGrid, tous les nœuds pxGrid doivent faire confiance aux certificats utilisés pour le connecteur Cisco Secure Workload ISE.

Étape 9 En utilisant les noms de fichiers de l'exemple ci-dessus, copiez le certificat client ISE - example-connector.pem, la clé du client - example-connector.key et l'autorité de certification – root-ca.example.com.pem dans les champs respectifs de la page de configuration ISE sur Cisco Secure Workload comme indiqué ci-dessous.

Note Avant de mettre à niveau vers la dernière version de Cisco Secure Workload, veillez à supprimer le connecteur ISE pour supprimer toutes les données de configuration existantes. Une fois la mise à niveau terminée, configurez le connecteur ISE avec les nouveaux filtres que vous souhaitez appliquer.

Figure 75: Configuration du connecteur ISE

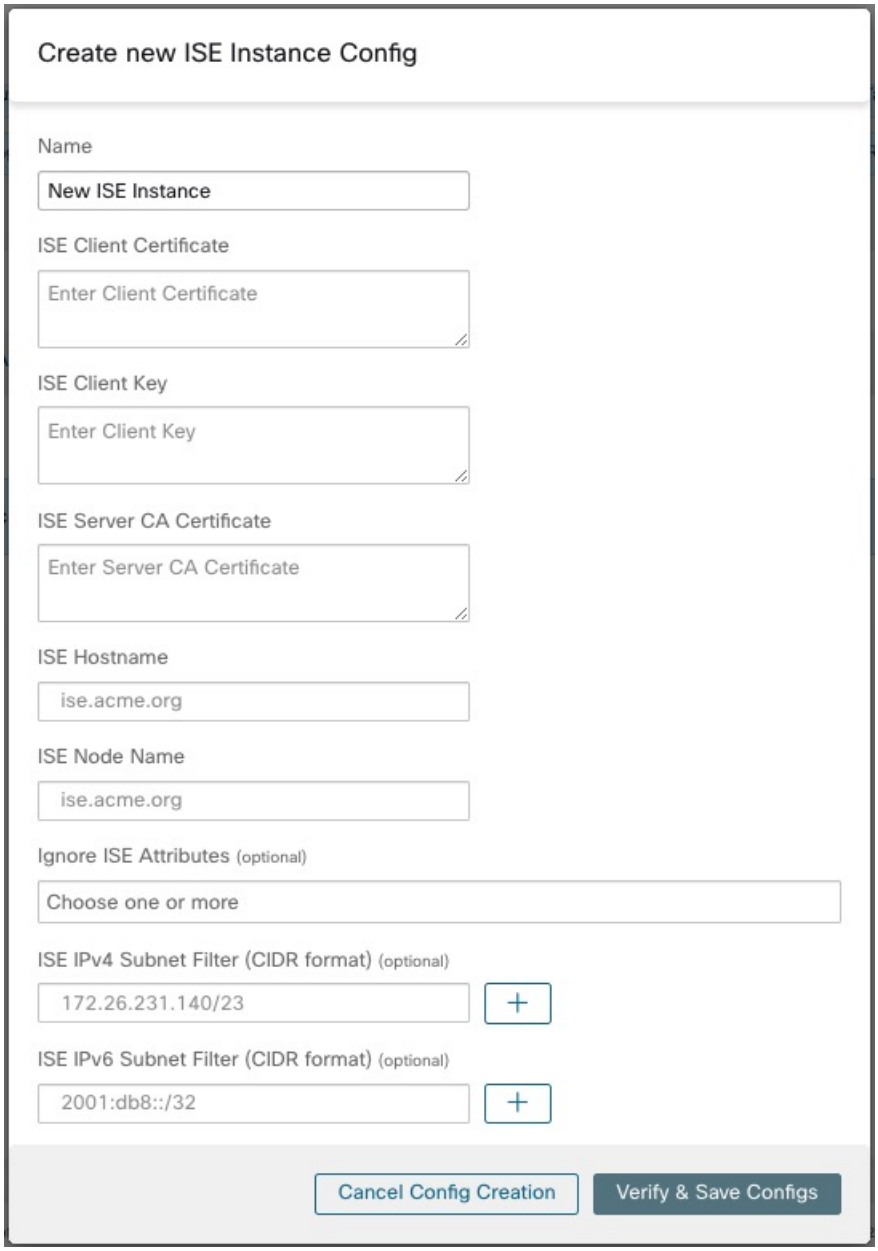


Table 18: Configuration du connecteur ISE

Champ	Description
Nom	Saisissez un nom d'instance ISE.
Certificat client ISE	Copiez et collez le certificat client ISE.

Champ	Description
Clé de client ISE	Copiez et collez la clé client ISE. La clé client doit être une clé en clair, qui n'est pas protégée par un mot de passe.
Certificat de l'autorité de certification du serveur ISE	Copiez et collez le certificat de l'autorité de certification racine.
Nom d'hôte ISE	Saisissez le nom d'hôte ISE (nom de domaine complet).
Nom de nœud ISE	Saisissez un nom de nœud
Ignorer les attributs ISE (facultatif)	Sélectionnez un ou plusieurs attributs ISE dans la liste. Utilisez cette option si vous ne souhaitez pas intégrer toutes les informations contextuelles des points terminaux signalés par le biais d'ISE.
Filtre de sous-réseau IPv4 ISE (format CIDR) (facultatif)	Saisissez plusieurs sous-réseaux IPv4 pour filtrer les points terminaux ISE.
Filtre de sous-réseau IPv6 ISE (format CIDR) (facultatif)	Saisissez plusieurs sous-réseaux IPv6 pour filtrer les points terminaux ISE.

Note

- Si une adresse IP est utilisée au lieu d'un nom de domaine complet pour le nom d'hôte ISE, utilisez l'adresse IP dans le SAN du certificat de l'autorité de certification ISE, sinon des échecs de connexion pourraient se produire.
- Le nombre de points terminaux actifs sur ISE n'est pas un instantané, il dépend des configurations sur ISE et de la durée d'agrégation pour le calcul de la mesure. Le nombre d'agents sur Cisco Secure Workload est toujours un instantané basé sur la dernière récupération de mises à jour d'ISE et de pxgrid, généralement le nombre de périphériques actifs au cours de la dernière journée (la fréquence d'actualisation par défaut des instantanés complets est d'un jour). En raison de la différence dans la façon dont ces nombres sont représentés, il est possible qu'ils ne correspondent pas toujours.

Traitement des enregistrements ISE

Le connecteur ISE traite les enregistrements comme décrit ci-dessous.

Enregistrement de point terminal

Le connecteur ISE se connecte à l'instance ISE et s'abonne à toutes les mises à jour des points terminaux sur pxGrid. Lors de la réception d'un enregistrement de point terminal, le connecteur ISE enregistre ce point terminal en tant qu'agent ISE sur Cisco Secure Workload. Le connecteur ISE utilise les informations spécifiques au point terminal présentes dans l'enregistrement de ce dernier ainsi que le certificat du connecteur ISE pour enregistrer le point terminal. Une fois qu'un point terminal est enregistré. Le connecteur ISE utilise l'objet de point terminal pour l'enrichissement de l'inventaire en l'envoyant en tant qu'étiquettes d'utilisateur sur

Cisco Secure Workload. Lorsque le connecteur ISE reçoit un point terminal déconnecté d'ISE, il supprime l'enrichissement d'inventaire de Cisco Secure Workload.

Enregistrement de groupe de sécurité

ISE connect s'abonne également aux mises à jour sur les modifications des étiquettes de groupes de sécurité via pxGrid. Lors de la réception de cet enregistrement, les connecteurs ISE conservent une base de données locale. ISE utilise cette base de données pour mapper le nom SGT avec la valeur lors de la réception d'un enregistrement de point terminal.

Tâches périodiques

Le connecteur ISE partage régulièrement des étiquettes d'utilisateur sur les inventaires de points terminaux ISE.

1. **instantanés de points terminaux** : toutes les 20 heures, le connecteur ISE récupère un instantané des points terminaux et des étiquettes de groupes de sécurité de l'instance ISE et met à jour la grappe si des modifications sont détectées. Cet appel ne tient pas compte des points terminaux déconnectés au cas où nous ne verrions pas de points terminaux sur Cisco Secure Workload en provenance d'ISE.
2. **Étiquettes d'utilisateur** : toutes les deux minutes, le connecteur ISE balaye les étiquettes d'utilisateur LDAP et de point terminal ISE gérées localement et met à jour les étiquettes d'utilisateur sur ces adresses IP.

Pour les étiquettes d'utilisateur, le connecteur ISE crée un instantané local des attributs LDAP de tous les utilisateurs de l'organisation. Lorsque le connecteur ISE est activé, la configuration LDAP (informations sur le serveur/port, attributs à récupérer pour un utilisateur, attribut qui contient le nom d'utilisateur) peut être fournie. De plus, les renseignements d'authentification de l'utilisateur LDAP pour accéder au serveur LDAP peuvent être fournis. Les informations d'authentification des utilisateurs LDAP sont chiffrées et ne sont jamais révélées dans le connecteur ISE. Si vous le souhaitez, un certificat LDAP peut être fourni pour un accès sécurisé au serveur LDAP.

Note Le connecteur ISE crée un nouvel instantané LDAP local toutes les 24 heures. Cet intervalle est configurable dans la configuration LDAP du connecteur.

Note Lors de la mise à niveau d'un périphérique Cisco ISE, le connecteur ISE devra être reconfiguré avec les nouveaux certificats générés par ISE après la mise à niveau.

Limites

Unité	Limite
Nombre maximal d'instances ISE qui peuvent être configurées sur un connecteur ISE	20
Nombre maximal de connecteurs ISE sur un appareil de périphérieCisco Secure Workload	1
Nombre maximal de connecteurs ISE sur un détenteur (portée racine)	1

Unité	Limite
Nombre maximal de connecteurs ISE sur Cisco Secure Workload	150

Connecteurs pour l'enrichissement de l'inventaire

Les connecteurs pour l'enrichissement de l'inventaire fournissent des métadonnées et du contexte supplémentaires sur les inventaires (adresses IP) surveillés par Cisco Secure Workload.

Connecteur	Description	Déployé sur une appliance virtuelle
ServiceNow	Recueillez des renseignements sur le point terminal de l'instance ServiceNow et enrichissez l'inventaire avec les attributs ServiceNow	Cisco Secure Workload Edge
Consultez aussi :	connecteurs infonuagiques	–

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs.

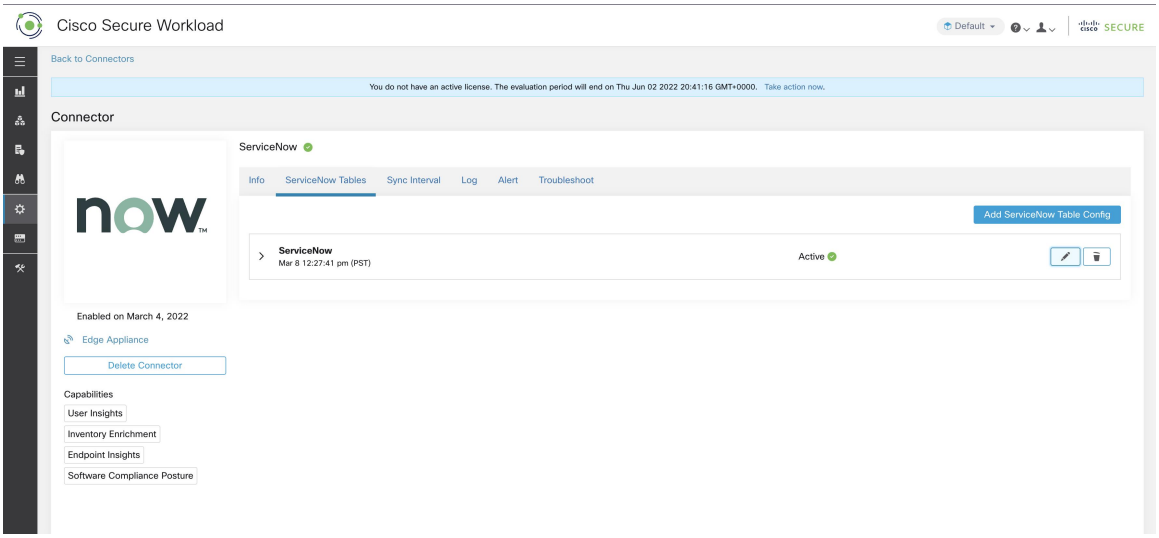
Connecteur ServiceNow

Le connecteur ServiceNow se connecte à l'instance ServiceNow pour obtenir toutes les étiquettes liées à la CMDB ServiceNow pour les points terminaux de l'inventaire ServiceNow. En utilisant cette solution, nous pouvons obtenir des métadonnées améliorées pour les points terminaux dans Cisco Secure Workload.

Le connecteur ServiceNow effectue les fonctions principales suivantes.

1. Mettre à jour les métadonnées ServiceNow dans l'inventaire de Cisco Secure Workload pour ces points terminaux.
2. Prendre régulièrement des instantanés et mettre à jour les étiquettes sur ces points terminaux.

Figure 76: Connecteur ServiceNow



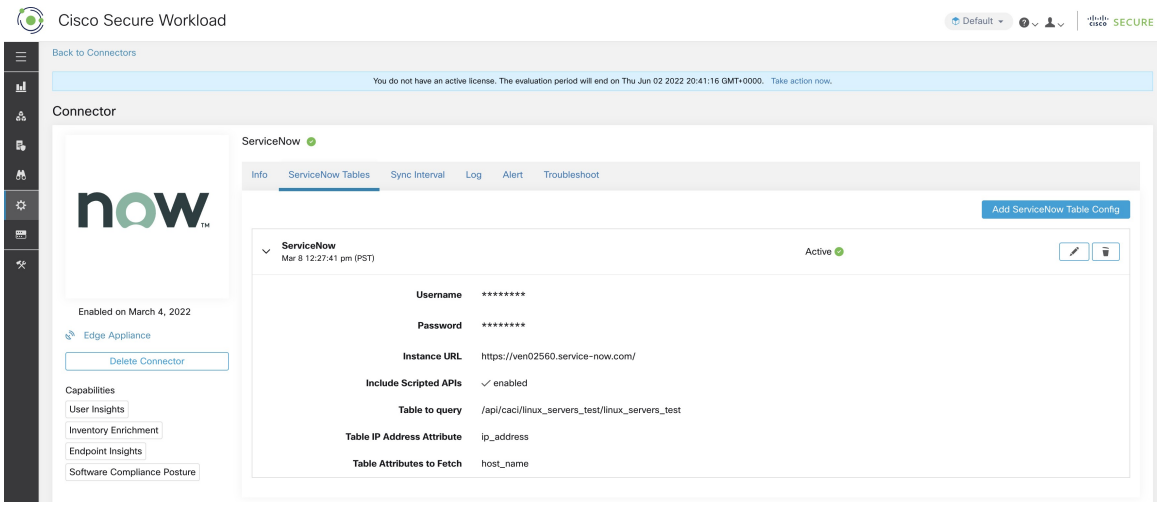
Comment configurer le connecteur ServiceNow

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *ServiceNow Tables* : la fonction ServiceNow Tables configure l'instance ServiceNow avec ses informations d'authentification et les informations sur les tables ServiceNow dans lesquelles récupérer les données.
- *API REST scriptée* : les tableaux de l' API REST scriptée ServiceNow peuvent être configurés de la même manière que les tableaux ServiceNow.
- *Sync Interval* : la configuration de l'intervalle de synchronisation permet de modifier la fréquence à laquelle Cisco Secure Workload doit interroger l'instance de ServiceNow pour obtenir des données mises à jour.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

Configuration de l'instance ServiceNow

Figure 77: Configuration de l'instance ServiceNow



Vous aurez besoin des éléments suivants pour configurer avec succès une instance ServiceNow.

1. Nom d'utilisateur ServiceNow
2. Mot de passe ServiceNow
3. URL de l'instance ServiceNow
4. Inclure les API scriptées

Par la suite, Cisco Secure Workload effectue une découverte de tous les tableaux à partir de l'instance ServiceNow et des API REST scriptées (uniquement si la case Include Scripted APIs (Inclure les API scriptées) est cochée). Il présente à l'utilisateur la liste des tableaux parmi lesquels choisir. Une fois qu'un utilisateur a sélectionné un tableau, Cisco Secure Workload récupère toute la liste des attributs de ce tableau pour que l'utilisateur puisse les sélectionner. L'utilisateur doit choisir l'attribut ip_address dans le tableau comme clé. Ensuite, l'utilisateur peut choisir jusqu'à 10 attributs uniques dans le tableau. Consultez les figures suivantes pour chaque étape.

Note Le connecteur ServiceNow peut uniquement prendre en charge l'intégration avec des tableaux comportant un champ d'**adresse IP**.

Note Pour intégrer les API REST scriptées de ServiceNow, vous devez cocher la case API scriptées, ce qui vous donnerait un flux de travail similaire à tout autre tableau.

Note Pour que les API REST scriptées s'intègrent au connecteur ServiceNow, elles ne peuvent pas avoir de paramètres de chemin. En outre, elles doivent prendre en charge **sysparm_limit,sysparm_fields and sysparm_offset** en tant que paramètres de requête.

Note Les rôles d'utilisateur ServiceNow doivent inclure **cmdb_read** pour les tableaux et **web_service_admin** pour les API REST scriptées afin de s'intégrer à Cisco Cisco Secure Workload.

Figure 78: Première étape de la configuration de l'instance ServiceNow

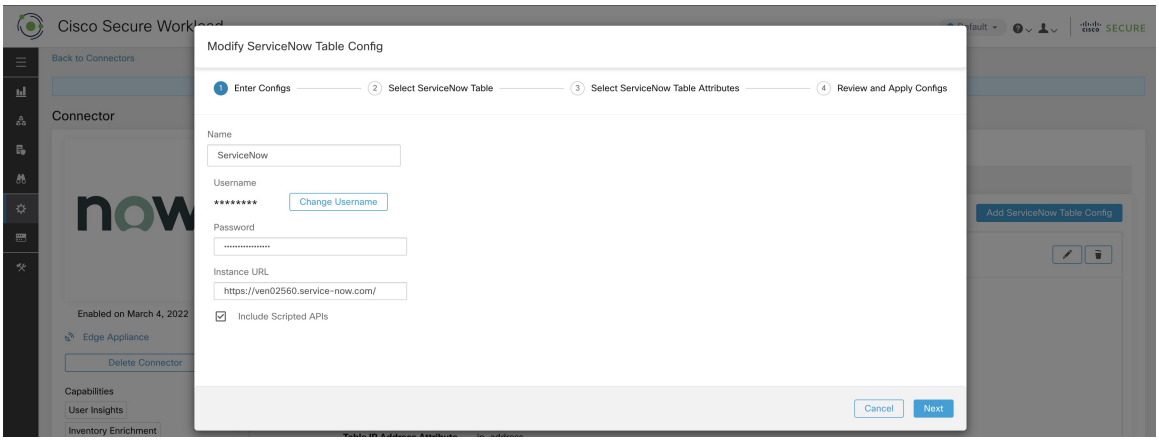


Figure 79: Cisco Secure Workload récupère les informations relatives aux tableaux de l'instance ServiceNow

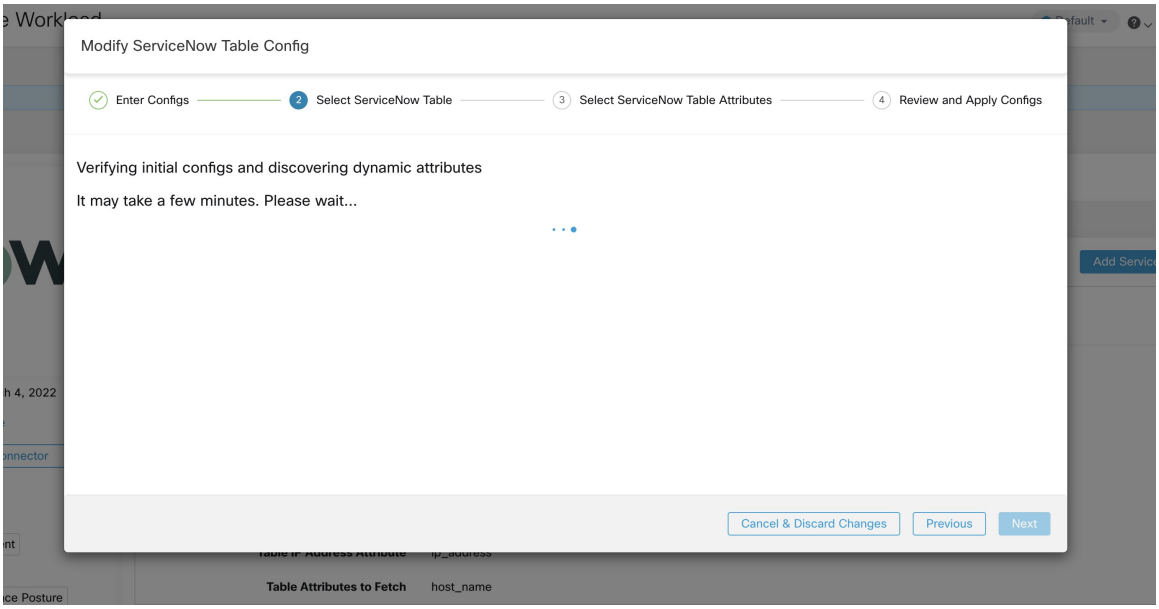


Figure 80: Cisco Secure Workload présente la liste des tableaux

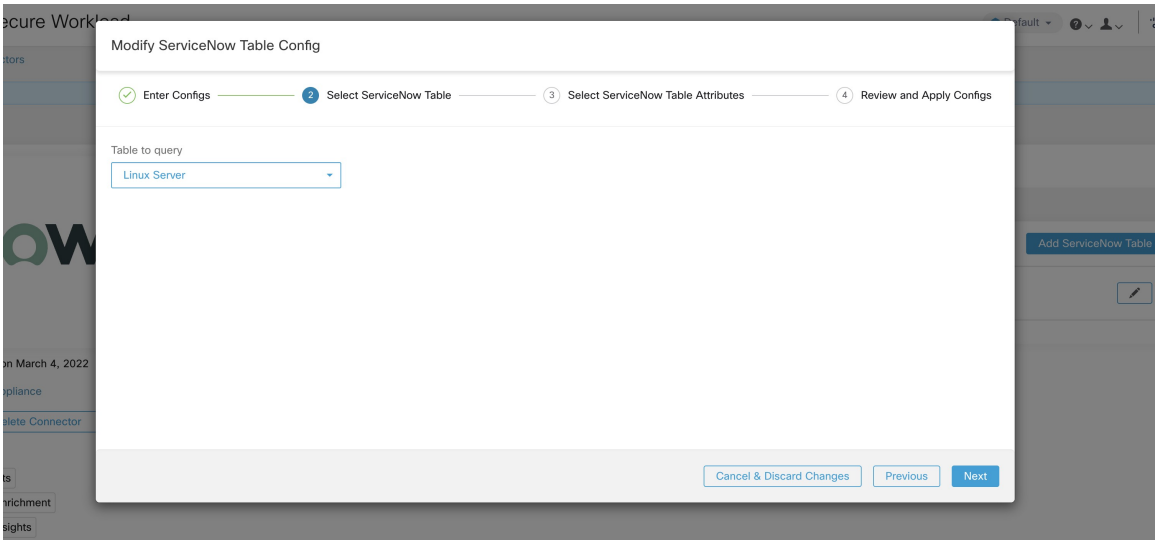


Figure 81: L'utilisateur sélectionne l'attribut ip_address et un autre attribut dans le tableau.

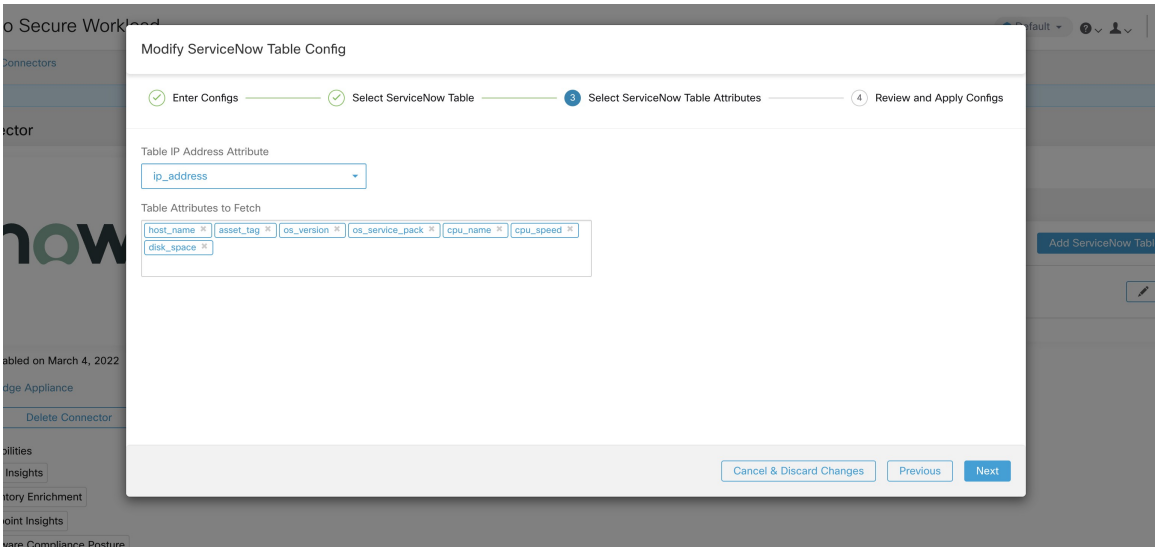
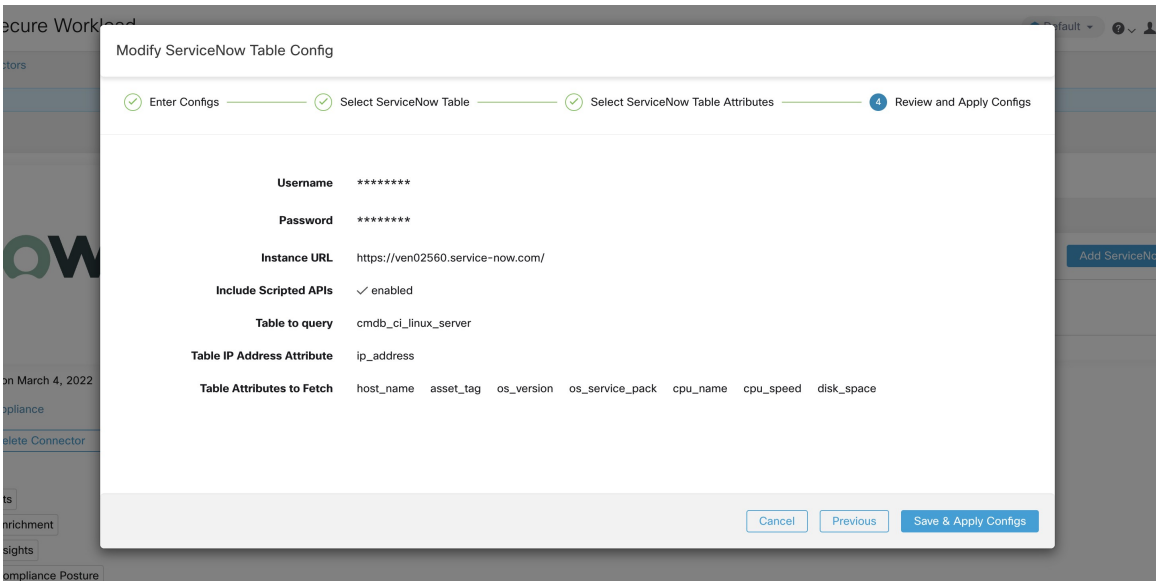


Figure 82: L'utilisateur finalise la configuration de ServiceNow.



Traitement des enregistrements ServiceNow

En fonction de l'URL d'instance que vous avez fournie lors de la configuration, le connecteur ServiceNow se connecte à l'instance ServiceNow. L'instance ServiceNow utilise des appels HTTP utilisant `https://{URL de l'instance}/api/new/doc/table/schema` pour obtenir le schéma de table initial à partir de l'API de la table ServiceNow. En fonction des tables configurées, il interroge ces tables pour récupérer les étiquettes et les métadonnées de ServiceNow. Cisco Secure Workload annote les étiquettes ServiceNow des adresses IP de son inventaire. Le connecteur ServiceNow récupère régulièrement de nouvelles étiquettes et met à jour l'inventaire Cisco Secure Workload .

Note Cisco Secure Workload récupère régulièrement les enregistrements des tables ServiceNow. Cela est configurable sous l'onglet SyncInterval dans le connecteur ServiceNow. L'intervalle de synchronisation par défaut est de 60 minutes. Pour les cas d'intégration de la table ServiceNow avec un grand nombre d'entrées, cet intervalle de synchronisation doit être défini à une valeur plus élevée.

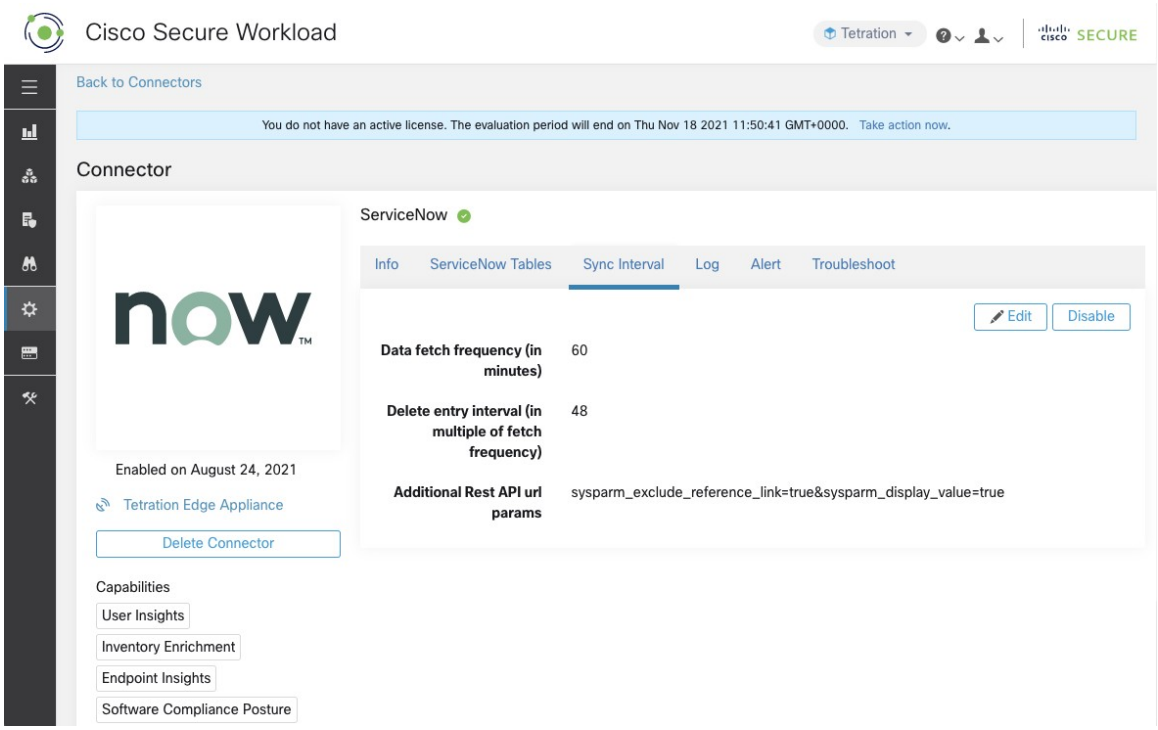
Note Cisco Secure Workload supprimera toute entrée non visible pendant 10 intervalles de synchronisation continus. Si la connexion à l'instance ServiceNow est interrompue pendant une période aussi longue, cela peut entraîner le nettoyage de toutes les étiquettes de cette instance.

Configuration de l'intervalle de synchronisation

1. Le connecteur ServiceNow de Cisco Secure Workload permet de configurer la fréquence de synchronisation entre Cisco Secure Workload et l'instance ServiceNow. Par défaut, l'intervalle de synchronisation est fixé à 60 minutes, mais il peut être modifié dans la configuration de l'intervalle de synchronisation sous la forme **Fréquence d'extraction des données**.

2. Pour détecter la suppression d'un enregistrement, le connecteur Cisco Secure Workload ServiceNow s'appuie sur les synchronisations des instances ServiceNow. Si une entrée n'est pas vue dans 48 intervalles de synchronisation consécutifs, nous supprimons l'entrée. Cela peut être configuré dans la configuration de l'intervalle de synchronisation sous la forme **Delete entry interval** (Supprimer l'intervalle d'entrée).
3. Si des paramètres supplémentaires doivent être transmis lors de l'appel des API REST pour les tableaux ServiceNow, vous pouvez les configurer dans le cadre des paramètres d'*URL supplémentaires de l'API REST*. Cette configuration est facultative. Par exemple, pour obtenir une recherche de référence à partir de ServiceNow, les paramètres d'URL suivants peuvent être utilisés **sysparm_exclude_reference_link=true&sysparm_display_value=vrai**

Figure 83: Configuration de l'intervalle de synchronisation



Commande Explore pour supprimer les étiquettes

Si l'utilisateur souhaite nettoyer les étiquettes pour une adresse IP particulière pour une instance donnée immédiatement, sans attendre l'intervalle de suppression, il peut le faire à l'aide de la commande explore. Voici les étapes à suivre pour exécuter la commande.

1. Recherche de l'ID VRF d'un détenteur
2. Accès à l'interface utilisateur de la commande Explore (Explorer)
3. Exécution des commandes

Recherche de l'ID VRF d'un détenteur

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Tenant** (Détenteur) sous le menu **platform** (plateforme) dans la barre de navigation à gauche de la

fenêtre. Cette page affiche tous les détenteurs et VRF actuellement configurés. Pour en savoir plus, consultez la section Détenteurs pour plus de détails.

Dans la page Détenteurs, le champ `ID` du tableau des détenteurs correspond à l'ID VRF du détenteur.

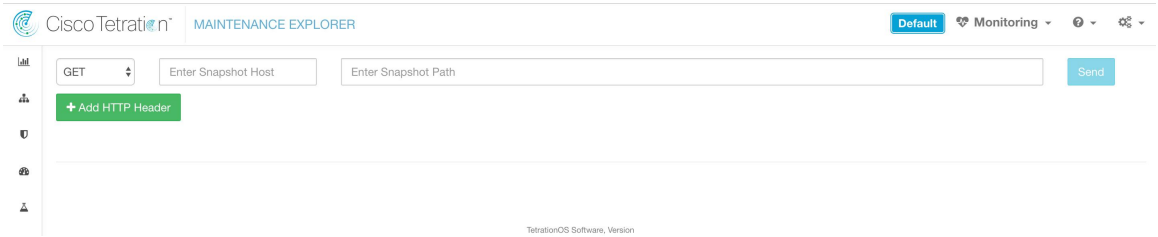
Accès à l'interface utilisateur de la commande Explore (Explorer)

Pour accéder à l'interface de commande Maintenance Explorer (Explorateur de maintenance), choisissez **Troubleshoot (Dépannage)** > **Maintenance Explorer (Explorateur de maintenance)** dans la barre de navigation de gauche de l'interface Web Cisco Secure Workload.

Note Des privilèges de service d'assistance à la clientèle sont nécessaires pour accéder au menu d'exploration. Si l'onglet d'exploration ne s'affiche pas, le compte n'a peut-être pas les autorisations nécessaires.

Cliquez sur l'onglet Explore (Explorer) dans le menu déroulant pour accéder à la page Maintenance Explorer (Explorateur de maintenance).

Figure 84: Onglet Maintenance Explorer (Explorateur de maintenance)



Exécution des commandes

- Choisissez l'action `POST`
- Saisissez l'hôte de l'instantané en tant que `orchestrator.service.consul`
- Saisir le chemin d'accès à l'instantané

  Pour supprimer les étiquettes d'une adresse IP particulière pour une `instance ServiceNow, procédez comme suit : servicenow_cleanup_annotations?args=<vrf-id> <ip_address> <instance_url> <table_name>`
- Cliquez sur Envoyer

Remarque Si, après avoir été supprimé à l'aide de la commande explore, l'enregistrement apparaît dans l'instance de ServiceNow, il sera réalimenté.

Foire aux questions

1. **Que faire si la table de CMDB ServiceNow ne comporte pas d'adresse IP.**

Dans ce cas, il est recommandé de créer une vue sur ServiceNow qui contiendra les champs souhaités de la table actuelle ainsi que l'adresse IP (provenant potentiellement d'une opération JOIN avec une autre table). Une fois qu'une telle vue est créée, elle peut être utilisée à la place du nom de table.

2. **Que se passe-t-il si l'instance ServiceNow nécessite une authentification multifactorielle**

   Actuellement, nous ne prenons pas en charge l'intégration de l'instance ServiceNow avec l'authentification multifactorielle.

Limites

Unité	Limite
Nombre maximal d'instances ServiceNow qui peuvent être configurées sur un connecteur ServiceNow	20
Nombre maximal d'attributs qui peuvent être extraits d'une instance de ServiceNow	10
Nombre maximal de connecteurs ServiceNow sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs ServiceNow sur un détenteur (portée racine)	1
Nombre maximal de connecteurs ServiceNow sur Cisco Secure Workload	150

Connecteurs pour les notifications d'alertes

Les connecteurs pour les notifications d'alertes permettent à Cisco Secure Workload de publier des alertes Cisco Secure Workload sur diverses plateformes de messagerie et de journalisation. Ces connecteurs fonctionnent sur le service TAN sur l'appareil de périphérie Cisco Secure Workload.

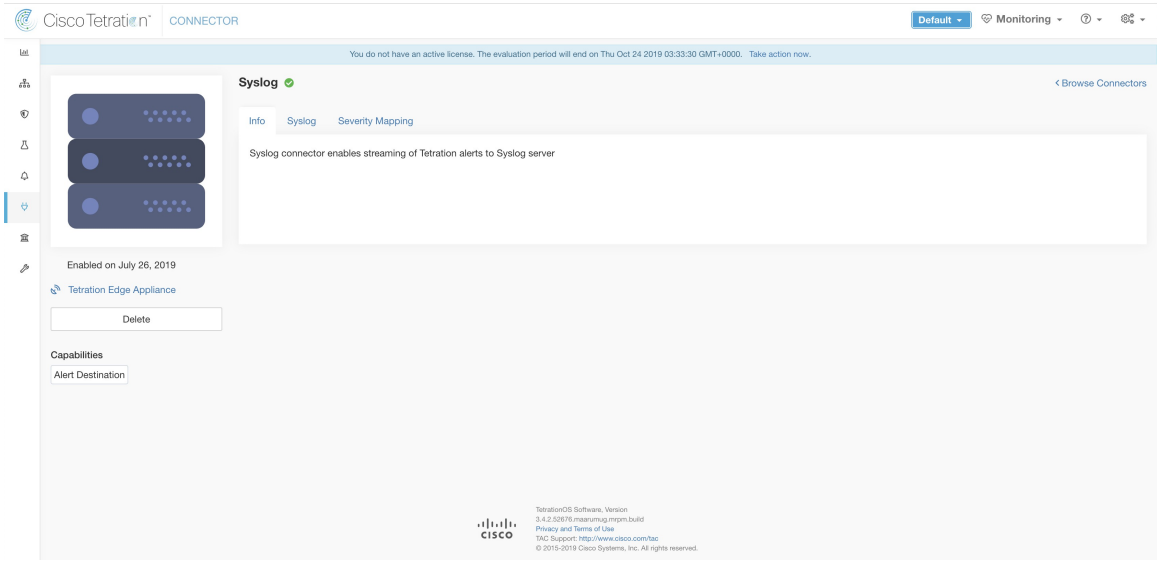
Connecteur	Description	Déployé sur une appliance virtuelle
Syslog	Envoyer des alertes Cisco Secure Workload au serveur Syslog.	Cisco Secure Workload Edge
Email	Envoyer des alertes Cisco Secure Workload par courriel	Cisco Secure Workload Edge
Slack	Envoyez des alertes Cisco Secure Workload sur Slack.	Cisco Secure Workload Edge
PagerDuty	Envoi d'alertes Cisco Secure Workload sur Pager Duty.	Cisco Secure Workload Edge
Kinesis	Envoyez des alertes Cisco Secure Workload sur Amazon Kinesis.	Cisco Secure Workload Edge

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

Connecteur Syslog

Lorsqu'activé, le service TAN (Outil de notification d'alertes) sur l'appareil de périphérie Cisco Secure Workload de Cisco peut envoyer des alertes au serveur Syslog à l'aide de la configuration.

Figure 85: Connecteur syslog



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur le serveur Syslog. Pour plus d'informations, consultez la Configuration de l'outil de notification Syslog.

Nom du paramètre	Type	Description
Protocol	Liste déroulante	Protocole à utiliser pour la connexion au serveur
	•*UDP*	
	• *TCP*	
Adresse du serveur	chaîne	Nom d'hôte ou adresse IP du serveur Syslog.
Port	number	Port d'écoute du serveur Syslog. La valeur du port par défaut est 514.

Figure 86: Exemple de configuration pour le connecteur Syslog

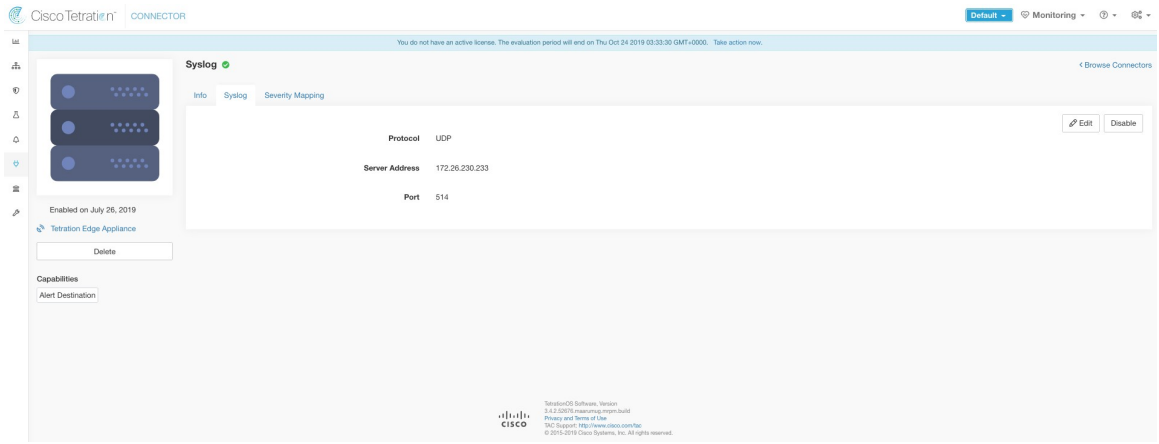


Figure 87: Exemple d'alerte

Mappage de gravité Syslog

Le tableau suivant présente le mappage de gravité par défaut pour les alertes Cisco Secure Workload dans Syslog.

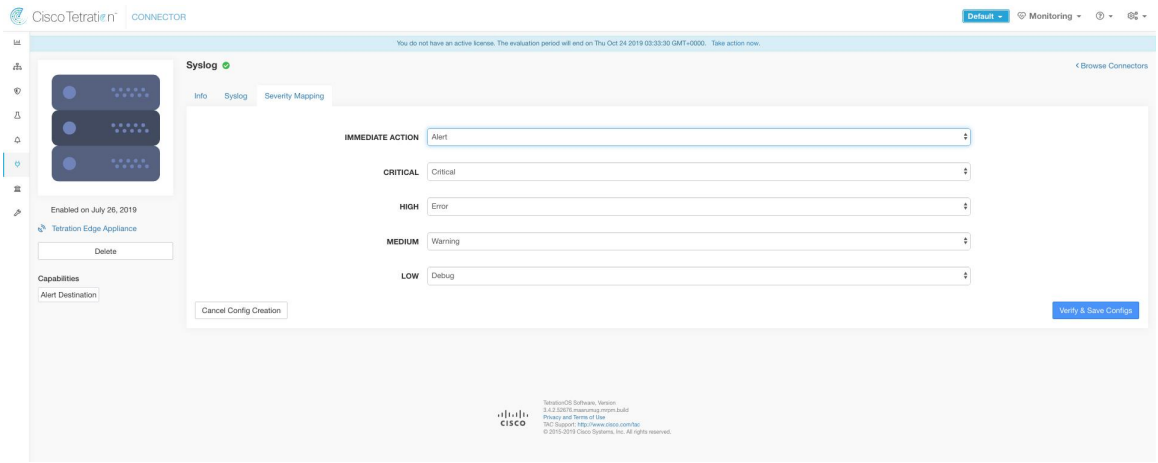
Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
FAIBLE	LOG_DEBUG
MOYENNE	LOG_WARNING
ÉLEVÉE	LOG_ERR
CRITIQUE	JOURNAL_CRIT

Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
ACTION IMMÉDIATE	LOG_EMERG

Ce paramètre peut être modifié à l'aide de la configuration du **Mappage de la gravité** du connecteur Syslog. Vous pouvez choisir la priorité Syslog correspondante pour chaque gravité d'alerte Cisco Secure Workload et modifier le mappage des gravités. Pour plus d'informations, consultez Configuration du mappage de gravité Syslog.

Nom du paramètre	Liste déroulante des mappages
ACTION_IMMÉDIATE	• *Urgence* • *Alerte* • *Critique* • *Erreur* • *Avertissement* • *Avis* • *Information* • *Débogage*
CRITIQUE	
ÉLEVÉ	
MOYENNE	
FAIBLE	

Figure 88: Exemple de configuration pour le mappage de gravité Syslog



Limites

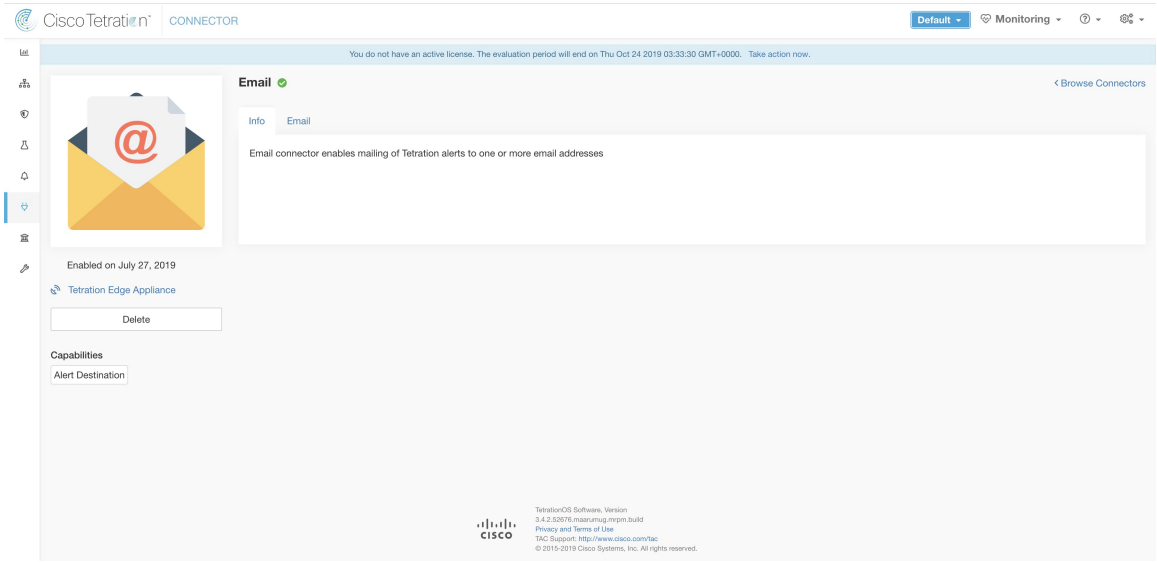
Unité	Limite
Nombre maximal de connecteurs Syslog sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Syslog sur un détenteur (portée racine)	1

Unité	Limite
Nombre maximal de connecteurs Syslog sur Cisco Secure Workload	150

Connecteur de courriel

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes pour une configuration donnée.

Figure 89: Connecteur de courriel



Le tableau suivant explique les détails de configuration pour la publication d'alertes Cisco Secure Workload dans des courriels. Pour en savoir plus, consultez la Configuration de l'outil de notification des courriels.

Table 19: Configuration du notificateur par courriel pour plus de détails

Nom du paramètre	Type	Description
Nom d'utilisateur SMTP	chaîne	Nom d'utilisateur du serveur SMTP Ce paramètre est facultatif.
Mot de passe SMTP	chaîne	Mot de passe du serveur SMTP pour l'utilisateur (si fourni) Ce paramètre est facultatif.
SMTP Server	chaîne	Nom d'hôte ou adresse IP du serveur SMTP
Port SMTP	number	Port d'écoute du serveur SMTP. La valeur par défaut est 587.
Connection sécurisée	case	Doit-on utiliser SSL pour la connexion au serveur SMTP?

Nom du paramètre	Type	Description
Adresse courriel d'expédition	chaîne	Adresse courriel à utiliser pour l'envoi des alertes
Destinataires par défaut	chaîne	Liste d'adresses courriel de destinataires séparées par des virgules

Figure 90: Exemple de configuration pour un connecteur par courriel

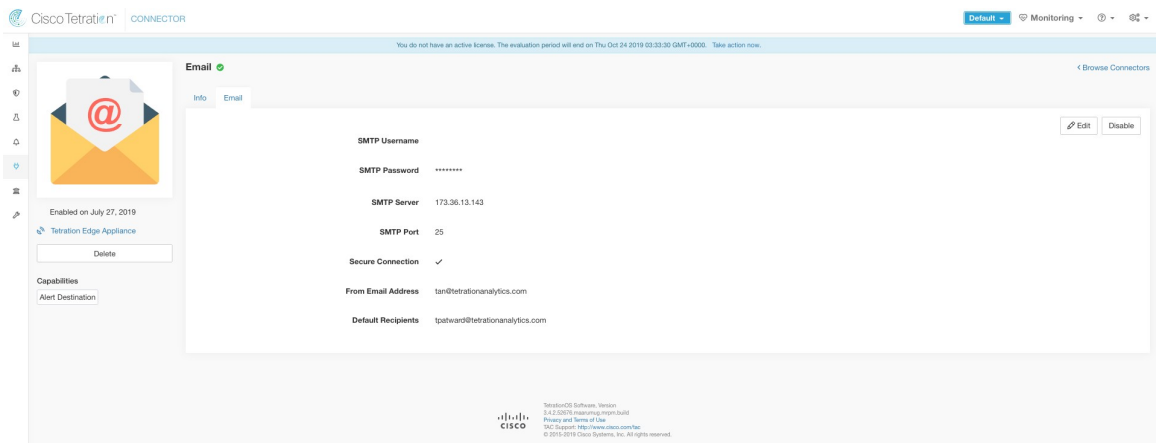
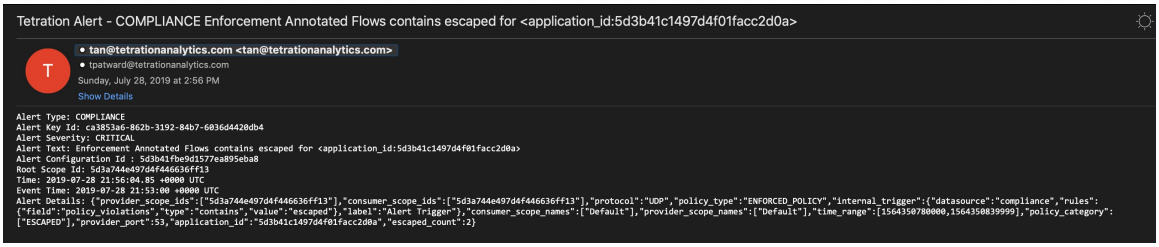


Figure 91: Exemple d'alerte



Note

- Le nom d'utilisateur et le mot de passe SMTP sont facultatifs. Si aucun nom d'utilisateur n'est fourni, nous essayons la connexion au serveur SMTP sans aucune authentification.
- Si la case de la connexion sécurisée n'est pas cochée, nous enverrons une notification d'alerte de connexion non sécurisée.
- La liste des destinataires par défaut est utilisée pour envoyer des notifications d'alertes. Cela peut être remplacé par alerte si la configuration des alertes l'exige.

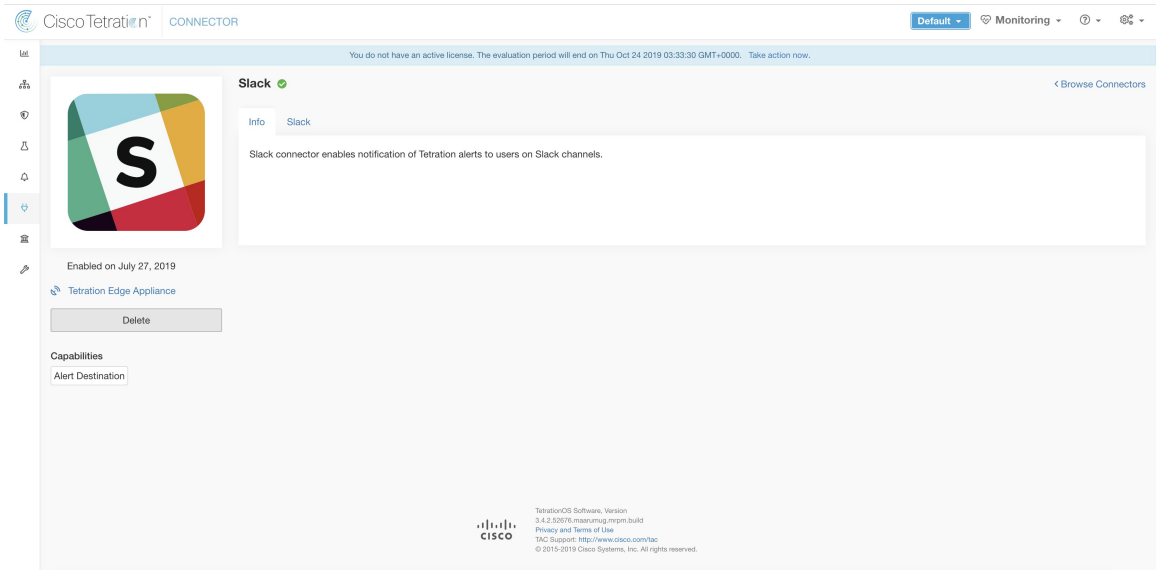
Limites

Unité	Limite
Nombre maximal de connecteurs de courriel sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs de courriel sur un détenteur (portée racine)	1
Nombre maximal de connecteurs de courriel sur Cisco Secure Workload	150

Connecteur Slack

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à Slack à l'aide de la configuration.

Figure 92: Connecteur Slack



Le tableau suivant explique les détails de la configuration pour la publication des alertes Cisco Secure Workload sur Slack. Pour en savoir plus, consultez la Configuration de l'outil de notification Slack.

Nom du paramètre	Type	Description
URL de point d'ancrage Web Slack	chaîne	Point d'ancrage Web Slack sur lequel les alertes Cisco Secure Workload doivent être publiées

Note

- Pour générer un point d'ancrage Web Slack, cliquez ici.

Figure 93: Exemple de configuration pour le connecteur Slack

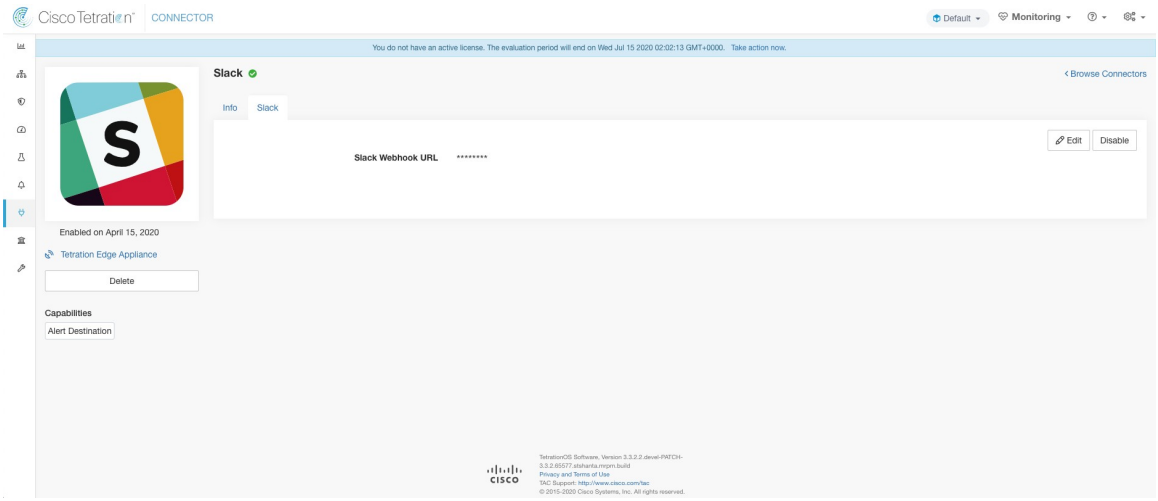
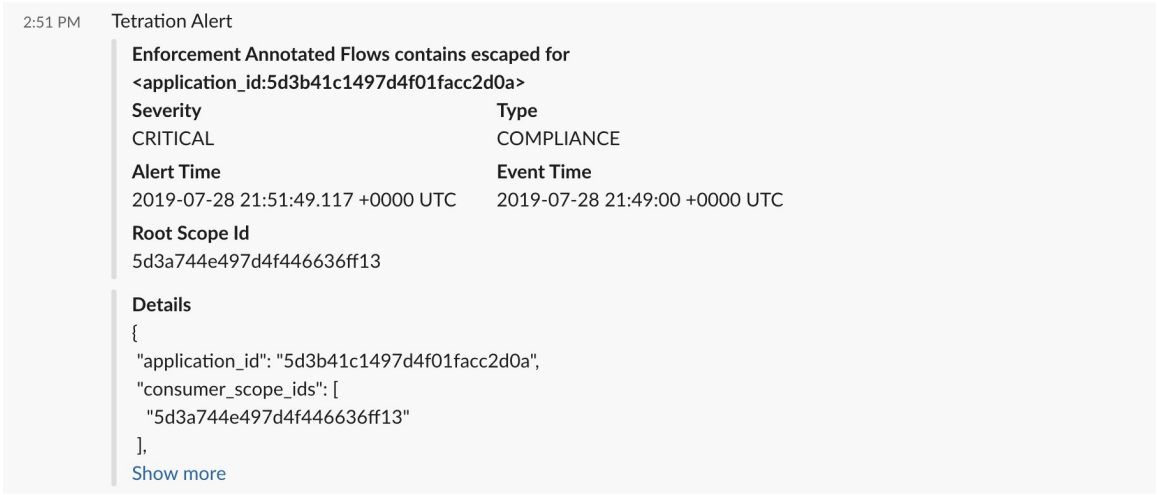


Figure 94: Exemple d'alerte



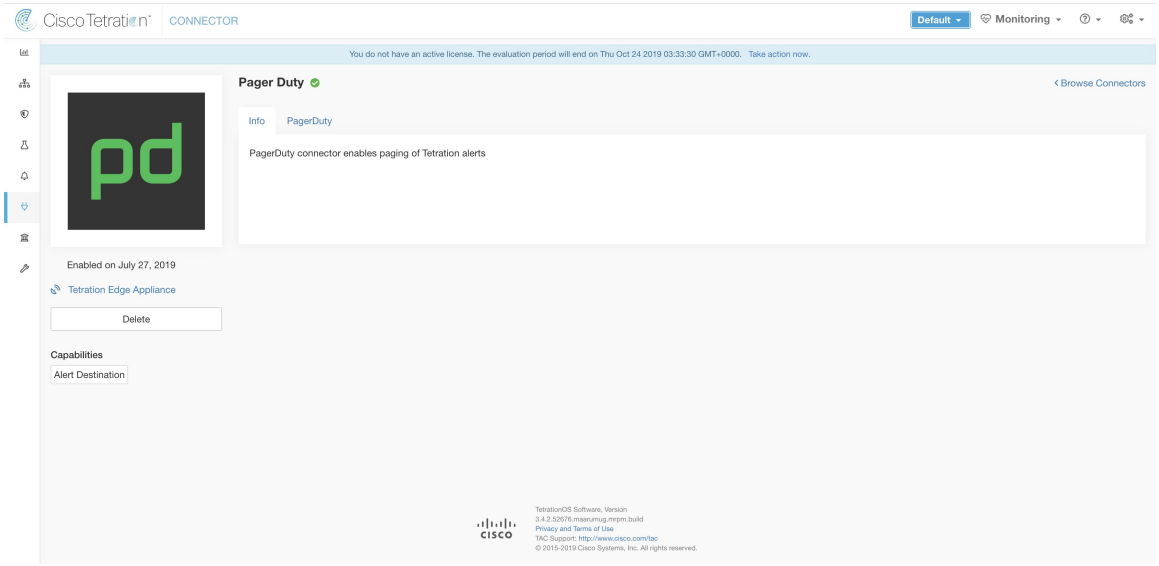
Limites

Unité	Limite
Nombre maximal de connecteurs Slack sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Slack sur un détenteur (portée racine)	1
Nombre maximal de connecteurs Slack sur Cisco Secure Workload	150

Connecteur PagerDuty

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à PagerDuty à l'aide de la configuration.

Figure 95: Connecteur PagerDuty



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur PagerDuty. Pour en savoir plus, consultez Configuration de l'outil de notification PagerDuty.

Nom du paramètre	Type	Description
Clé de service PagerDuty	chaîne	Clé de service PagerDuty pour activer les alertes Cisco Secure Workload sur PagerDuty.

Figure 96: Exemple de configuration pour PagerDuty Connector

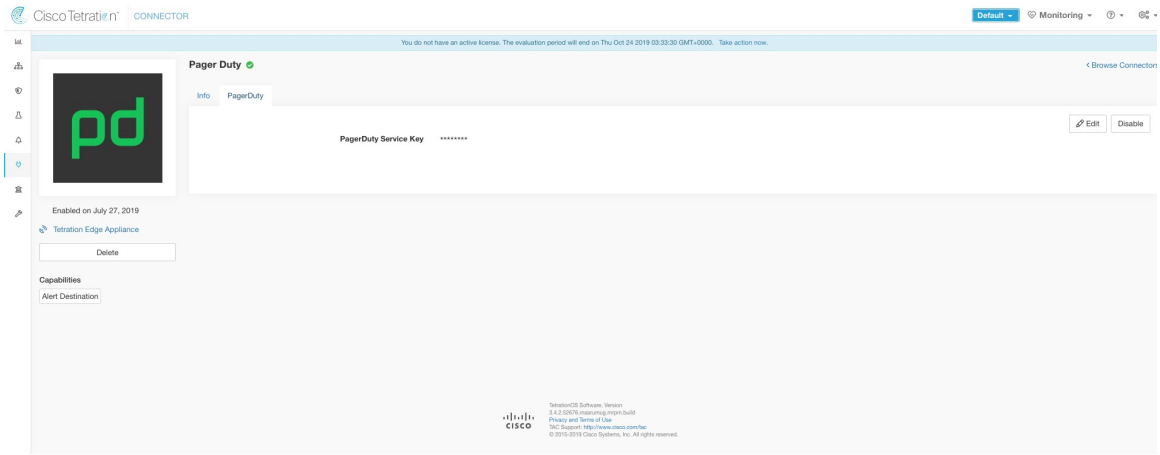
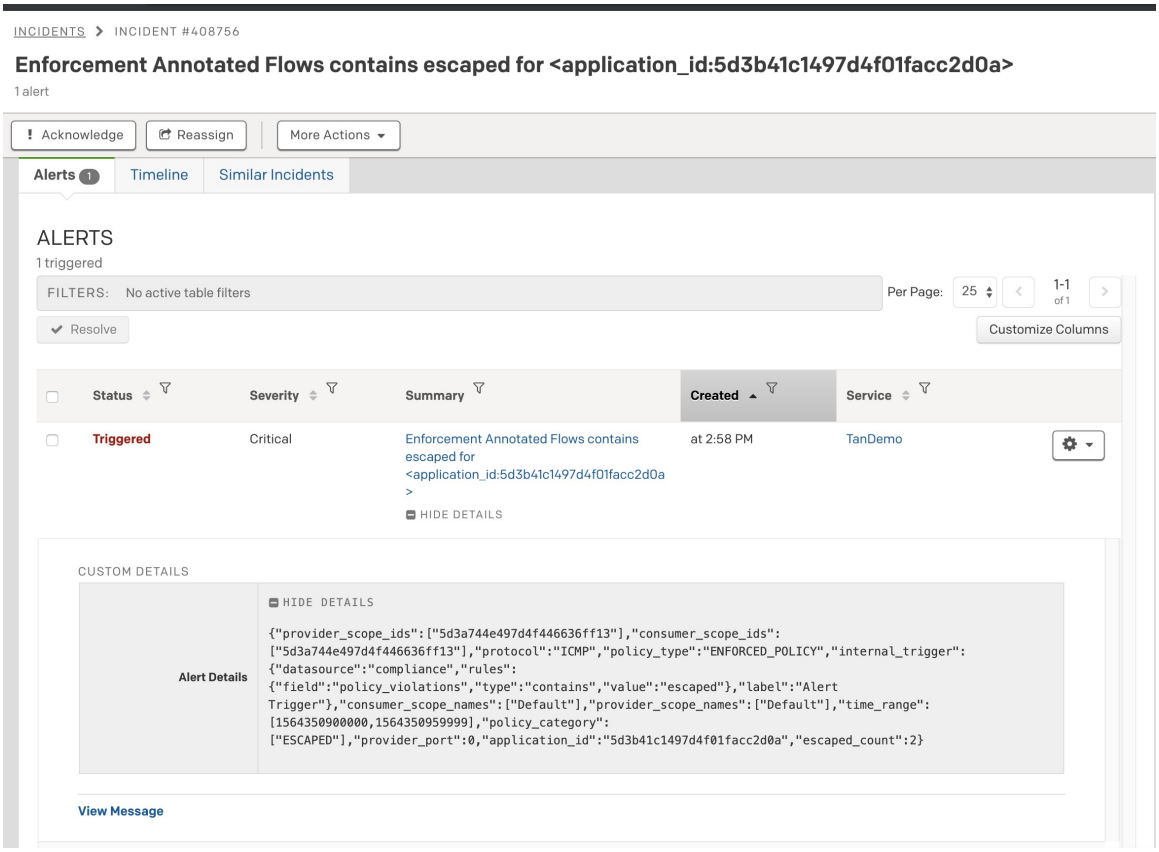


Figure 97: Exemple d'alerte



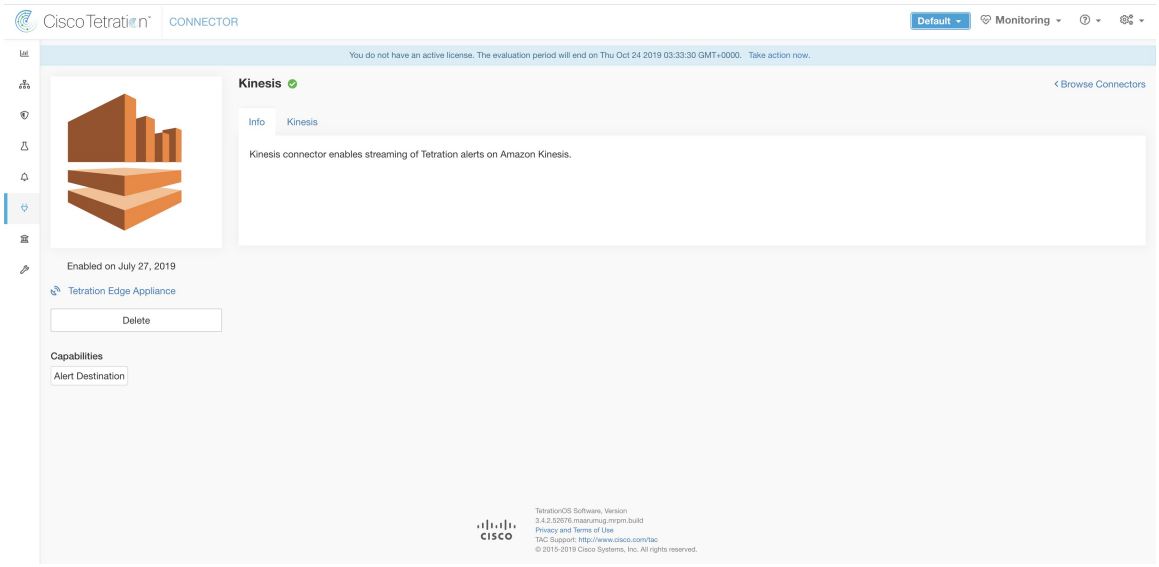
Limites

Unité	Limite
Nombre maximal de connecteurs PagerDuty sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs PagerDuty sur un détenteur (portée racine)	1
Nombre maximal de connecteurs PagerDuty sur Cisco Secure Workload	150

Connecteur Kinesis

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à l'aide de la configuration.

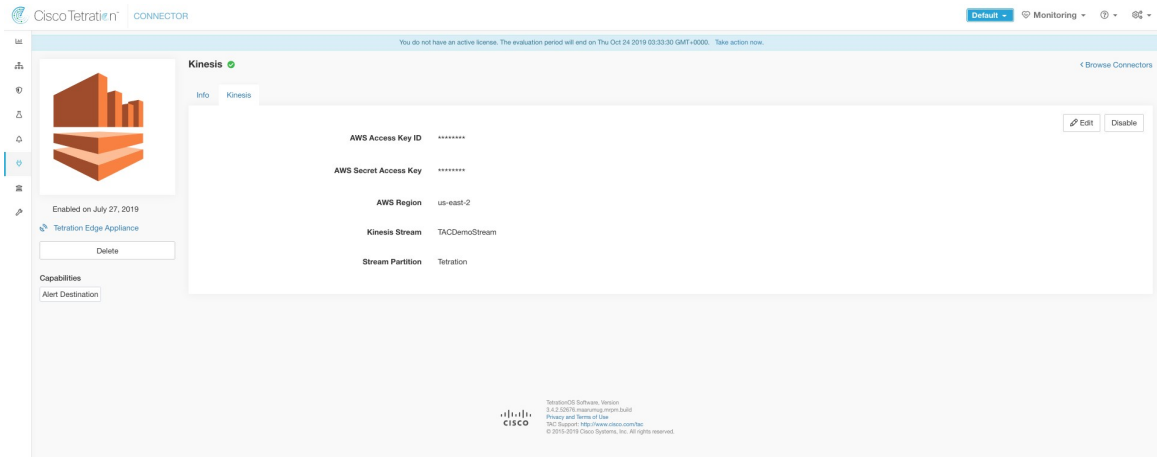
Figure 98: Connecteur Kinesis



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur Amazon Kinesis. Pour en savoir plus, consultez la Configuration de l'outil de notification Kinesis.

Nom du paramètre	Type	Description
ID de la clé d'accès AWS	chaîne	ID de clé d'accès AWS pour communiquer avec AWS
Clé d'accès secrète AWS	chaîne	Clé d'accès secrète AWS pour communiquer avec AWS
Région AWS	dropdown of AWS regions	Nom de la région AWS où le flux Kinesis est configuré
Kinesis Stream	chaîne	Nom du flux Kinesis
Stream Partition	chaîne	Nom de la partition du flux

Figure 99: Exemple de configuration pour le connecteur Kinesis



Limites

Unité	Limite
Nombre maximal de connecteurs Kinesis sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Kinesis sur un détenteur (portée racine)	1
Nombre maximal de connecteurs Kinesis sur Cisco Secure Workload	150

connecteurs infonuagiques

Vous pouvez utiliser un connecteur infonuagique pour les fonctionnalités Cisco Secure Workload sur les charges de travail infonuagique.

Les connecteurs infonuagiques ne nécessitent pas d'appliance virtuelle.

Connecteur	Fonctionnalités prises en charge	Déployé sur une appliance virtuelle
AWS	Pour les VPC Amazon Web Services : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes EKS (Elastic Kubernetes Service) : • Recueillir des métadonnées	S. O.
Azure	Pour les réseaux virtuels Azure : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes Azure Kubernetes Service (AKS) : • Recueillir des métadonnées	S. O.
GCP	Pour les VPC Google Cloud Platform : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes de Google Kubernetes Engine (GKE) : • Recueillir les métadonnées (étiquettes)	s.o.

Connecteur AWS

Le connecteur Amazon Web Services (AWS) se connecte à AWS pour remplir les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses étiquettes) en direct à partir d'un nuage privé virtuel (VPC)** AWS; AWS vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload interroger les balises de ces ressources qui peuvent ensuite être utilisées pour la visualisation des données d'inventaire et des flux de trafic, et pour la définition de politiques. Cette fonctionnalité maintient le mappage des balises de ressources à jour en synchronisant constamment ces données.

  Les balises des charges de travail et des interfaces réseau d'un AWS VPC sont acquises. Si vous configurez à la fois des charges de travail et des interfaces réseau, Cisco Secure Workload fusionne et affiche les balises. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques, on page 352.

- **Acquisition de journaux de flux VPC** Si vous avez configuré les journaux de flux VPC dans AWS à des fins de surveillance, Cisco Secure Workload peut acquérir des informations des journaux de flux en lisant le compartiment S3 correspondant. Vous pouvez utiliser cette télémétrie pour la génération de politiques de visualisation et de segmentation.

- **Segmentation** Lorsque l'option de segmentation est activée, Cisco Secure Workload programme les politiques de sécurité à l'aide des groupes de sécurité natifs d'AWS. Lorsque la mise en application est activée pour un VPC, les politiques pertinentes sont automatiquement programmées en tant que groupes de sécurité.

- **Acquisition automatisée des métadonnées des grappes EKS** Lorsque Elastic Kubernetes Services (EKS) est exécuté sur AWS, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et de pods associées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir les fonctionnalités à activer pour chaque VPC.

Note Nous ne prenons pas actuellement en charge les régions de la Chine.

Exigences et prérequis AWS

Pour toutes les fonctionnalités : créez un utilisateur dédié dans AWS ou identifiez un utilisateur AWS existant pour ce connecteur. L'assistant de configuration du connecteur génère un modèle de formation de nuage CloudFormation (CFT) que vous pouvez utiliser pour attribuer les privilèges requis à cet utilisateur. Assurez-vous que vous avez les autorisations dans AWS pour charger ce CFT.

Pour accorder un accès multicompte AWS à l'utilisateur dédié, consultez (Facultatif) Configurer l'accès multicompte AWS dans AWS, on page 243, y compris les privilèges d'accès requis.

Pour accorder l'accès au compte AWS à l'aide du rôle, consultez la section accès basé sur les rôles à la grappe Cisco Secure Workload.

Chaque VPC ne peut appartenir qu'à un seul connecteur AWS. Une grappe Cisco Secure Workload peut avoir plusieurs connecteurs AWS. Rassemblez les informations décrites dans les tableaux de la Configurer un nouveau connecteur AWS , on page 247.

Ce connecteur ne nécessite pas d'appliance virtuelle.

Pour la collecte d'étiquettes et de l'inventaire : aucune condition préalable supplémentaire n'est requise.

Pour l'acquisition des journaux de flux : des définitions de journaux de flux au niveau VPC sont requises pour déclencher la collecte des journaux de flux.

Seuls les journaux de flux de niveau VPC peuvent être intégrés.

Les journaux de flux doivent être publiés dans Amazon Simple Storage Service (S3). Cisco Secure Workload ne peut pas collecter de données de flux à partir des journaux Amazon CloudWatch.

Secure Workload peut acquérir des journaux de flux d'un compartiment S3 associé à n'importe quel compte, si les informations d'authentification du compte d'utilisateur AWS fournies lors de la création du connecteur ont accès à la fois aux journaux de flux VPC et au compartiment S3.

Les attributs de journal de flux suivants (dans n'importe quel ordre) sont requis dans ce dernier : adresse source, adresse de destination, port source, port de destination, protocole, paquets, octets, heure de début, heure de fin, action, indicateurs TCP, ID d'interface, État du journal et direction du flux. Tout autre attribut est ignoré.

Les journaux de flux doivent saisir le trafic autorisé et refusé.

Note Le connecteur Cisco Secure Workload AWS prend en charge la partition des journaux de flux VPC sur une base horaire et quotidienne.

Pour la segmentation : l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Sauvegardez vos groupes de sécurité existants avant d'activer la segmentation du connecteur, car toutes les règles existantes sont remplacées lorsque vous activez la segmentation pour un VPC.

Pour en savoir plus, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.

Pour les services Kubernetes gérés (EKS) : si vous activez l'option Kubernetes, consultez Exigences et prérequis EKS dans la section des services Kubernetes gérés fonctionnant sur AWS (EKS), y compris les privilèges d'accès requis.

(Facultatif) Configurer l'accès multicompte AWS dans AWS

Si les renseignements d'authentification utilisateur fournis ont accès aux VPC appartenant à d'autres comptes AWS, ces derniers seront disponibles pour traitement dans le cadre du connecteur AWS.

1. L'utilisateur Cisco Secure Workload désigné doit disposer des autorisations d'accès AWS suivantes :

```
1. iam:GetPolicyVersion
2. iam:ListPolicyVersions
3. iam:ListAttachedUserPolicies
4. iam:GetUser
5. servicequotas:ListServiceQuotas
```

Exemple JSON de politique AWS :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:ListPolicyVersions",
        "iam:ListAttachedUserPolicies",
        "iam:GetUser",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

2. Créez un rôle IAM AWS dans le compte AWS souhaité dont l'utilisateur Cisco Secure Workload désigné ne fait PAS partie.
3. Autorisez que le rôle AWS IAM soit assumé par l'utilisateur Cisco Secure Workload. Cela peut être fait en ajoutant l'ARN de l'utilisateur Cisco Secure Workload à la politique d'approbation du rôle IAM d'AWS.

   Exemple JSON de politique d'approbation de rôle IAM AWS :

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": <Secure Workload_user_arn>
            },
  "Action": "sts:AssumeRole",
  "Condition": {}
    }
  ]
}
```

4. Exécutez les étapes 2 et 3 pour tous les comptes AWS souhaités auxquels l'utilisateur Cisco Secure Workload n'appartient pas.
5. Créez une politique gérée par le client (PAS une politique en ligne) avec l'autorisation d'assumer tous les rôles AWS créés à partir de différents comptes.

Remarque Dans le connecteur AWS, la politique en ligne du client n'est pas prise en charge.

Exemple de politique gérée JSON :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [<AWS_role_cross_account_1_arn>, <AWS_role_cross_account_2_arn>...]
    }
  ]
}
```

6. Associez la politique gérée par le client créée à l'utilisateur Cisco Secure Workload.
7. L'assistant de configuration du connecteur fournit un modèle CloudFormation. Après avoir téléchargé la CFT telle quelle sur l'utilisateur Cisco Secure Workload désigné, vous modifierez le modèle et vous téléchargerez le modèle modifié sur le portail CloudFormation pour accorder les autorisations requises pour les rôles AWS IAM. Pour en savoir plus, consultez Configurer un nouveau connecteur AWS , à la page 247.

Authentification à l'aide de rôles

L'authentification basée sur l'utilisateur nécessite des clés d'authentification. Une clé d'authentification mal gérée peut constituer une menace pour la sécurité en raison de sa nature sensible.

L'utilisation de l'authentification basée sur les rôles vous permet de configurer le compte AWS à l'aide de rôles. La configuration du connecteur accepte l'identifiant du rôle (ARN) et assume ce rôle pour effectuer des actions spécifiques sur le compte du client.

L'authentification basée sur les rôles réduit le risque d'accès non autorisé.

Pour accéder à l'authentification basée sur les rôles, procédez comme suit :

Procédure

Étape 1 Cliquez sur l'onglet **Role** (Rôle) dans la page de configuration du connecteur.

Étape 2 Enregistrez la grappe. Si la grappe n'est pas enregistrée, elle affiche le message *« Cluster is not registered to use role credentials (La grappe n'est pas enregistrée pour utiliser les informations d'authentification du rôle) ». Téléchargez la charge utile fournie et communiquez avec un représentant du service d'assistance à la clientèle.*.

Étape 3 Dans le message de notification, cliquez sur le bouton de **Download** (Téléchargement) et téléchargez le fichier de charge utile.

Étape 4 Vous pouvez utiliser le lien dans le message de notification pour contacter l'équipe **TAC**, créer le dossier et fournir le fichier que vous avez téléchargé.

Étape 5 Lorsque la grappe est enregistrée, l' **ID externe** et **l'ARN de l'utilisateur** sont remplis automatiquement.

Remarque Actualisez la page pour afficher l'ID externe et l'ARN de l'utilisateur.

Étape 6 Utilisez l' **ID externe** et **l'ARN utilisateur** générés pour mettre à jour la relation d'approbation de rôle. Elle permet d'assumer le rôle.

La même partie du fichier JSON :

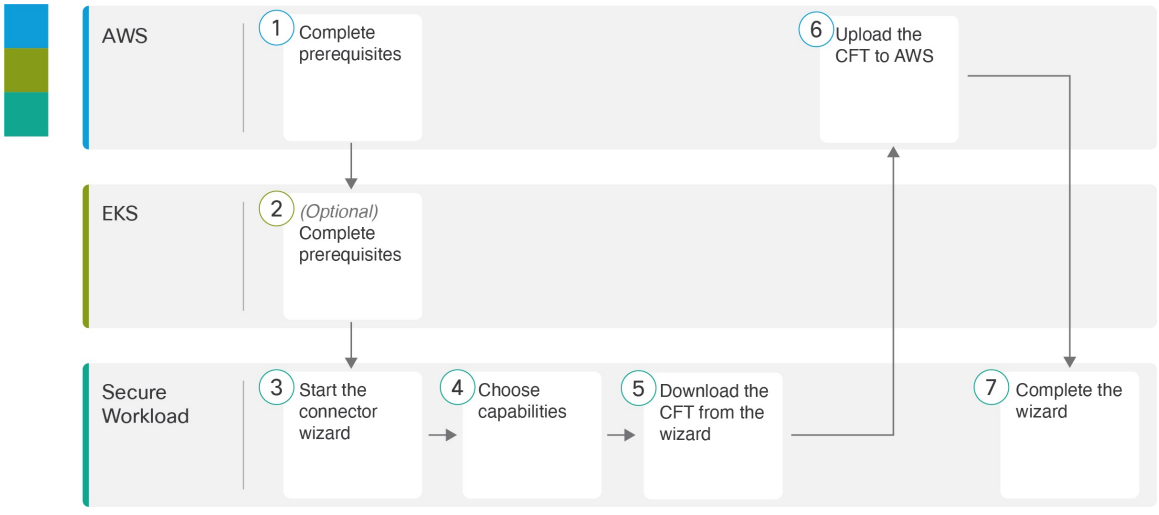
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "<User ARN>"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "<External Id>"
        }
      }
    }
  ]
}
```

Étape 7 Lorsque l'étape précédente est terminée, vous pouvez copier l' **ARN de rôle** du compte AWS et le coller dans la page de configuration du connecteur AWS.

Aperçu de la configuration du connecteur AWS

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour obtenir des renseignements essentiels, consultez la rubrique suivante (Configurer un nouveau connecteur AWS , à la page 247)

Illustration 100 : Aperçu de la configuration du connecteur AWS



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un nouveau connecteur AWS

Procédure

Étape 1 Dans le volet de navigation, choisissez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **AWS Connector** (Connecteur AWS).

Étape 3 Cliquez sur **Generate Template** (générer un modèle) et sélectionnez les fonctionnalités souhaitées.

En fonction des capacités sélectionnées, un modèle CloudFormation (FormationNuage) (CFT) est généré. Utilisez le modèle CFT généré dans votre CloudFormation AWS pour créer la politique pour l'utilisateur ou le rôle.

Pour activer la segmentation, vous devez également cocher**Gather Labels** (Regrouper les étiquettes).

Étape 4 Téléchargez le modèle CloudFormation (CFT) généré. Le CFT généré peut être utilisé à la fois pour l'utilisateur et le rôle.

Ce modèle dispose des privilèges IAM requis pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option Kubernetes, vous devez configurer séparément les autorisations pour EKS. Consultez Services gérés Kubernetes s'exécutant sur AWS (EKS), à la page 253.

Étape 5 Chargez le CFT sur le portail AWS CloudFormation pour attribuer des privilèges à l'utilisateur pour ce connecteur. Assurez-vous que l'utilisateur AWS dispose des privilèges requis avant de pouvoir continuer la configuration du connecteur AWS.

Remarque Nous vous recommandons d'effectuez cette opération, que vous utilisiez ou non l'accès entre comptes AWS.

Vous pouvez appliquer le CFT à l'aide du portail ou de la CLI. Pour en savoir plus, consultez ;

- **Portail :** AWS Management Console
- **CLI :** Création d'une pile

Lorsque vous chargez le CFT, AWS exige les détails suivants :

1. Nom de la politique (il peut s'agir de n'importe quel nom. Par exemple, connecteur Cisco Secure Workload)
2. Nom du rôle : nom du rôle IAM AWS auquel vous appliquez le CFT
3. Liste des ARN de compartiment et des ARN d'objet (par défaut : *)
4. Nom de l'utilisateur : nom de l'utilisateur AWS auquel vous appliquez le CFT
5. Liste des ARN de VPC (par défaut : *)

   Pour saisir une liste spécifique d'ARN de VPC, saisissez les ressources du groupe de sécurité et de l'interface réseau jumelées avec le VPC spécifique pour activer la segmentation.

   1. `arn:aws:ec2:<region>:<account_id>:security-group/*`
   2. `arn:aws:ec2:<region>:<account_id>:network-interface/*`

Exemple de code

Exemple 1

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:us-east-1:123456789:security-group/*",
    "arn:aws:ec2:us-east-1:123456789:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

Exemple 2

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

Étape 6 Si vous utilisez l'authentification basée sur les rôles d'AWS pour vous connecter au connecteur Cisco Secure Workload, consultez la section Rôles et privilèges d'accès EKS.

Étape 7 Si vous utilisez l'accès entre comptes AWS, suivez ces étapes supplémentaires :

1. Vous pouvez utiliser le même CFT téléversé pour donner accès au rôle ou à l'utilisateur. Si vous avez plusieurs comptes, utilisez le même CFT pour chaque compte.
2. Chargez le CFT dans le portail AWS CloudFormation de chaque compte AWS pour lequel le rôle IAM souhaité existe.

   Vous pouvez appliquer le CFT à l'aide du portail ou de la CLI, comme décrit à l'étape précédente.

   Lorsque vous chargez le CFT, AWS demande ce qui suit :

   1. Nom de la politique (il peut s'agir de n'importe quel nom. Par exemple, connecteur Cisco Secure Workload)
   2. Liste des ARN de compartiment et des ARN d'objet (par défaut : *)

3. Nom du rôle : nom du rôle IAM AWS auquel vous appliquez le CFT
4. Liste des ARN de VPC (par défaut : *)

Étape 8 Cliquez sur **Getting Started guide** (Guide de démarrage, recommandé) ou sur le bouton **Configure your new connector here** (configurer votre nouveau connecteur ici) pour configurer le connecteur.

Étape 9 Comprenez et respectez les Exigences et prérequis AWS, et Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, puis cliquez sur **Get Started** (Démarrer). Ou, si vous effectuez la configuration à l'aide du bouton **Configure your new connector**, (Configurer votre nouveau connecteur) cliquez sur **yes** (oui).

Étape 10 Nommez le connecteur et saisissez la description.

Étape 11 Configurer les paramètres :

Vous pouvez utiliser l'une ou l'autre de ces options pour vous connecter au compte AWS.

1. Clés d'authentification
2. Rôles

Nom du paramètre	Attribut	Description
Clés d'authentification	Access Key	ID de la CLÉ d'accès associé à l'utilisateur AWS qui dispose des privilèges décrits dans le CFT ci-dessus.
	Secret Key	CLÉ SECRÈTE associée à l'ID de la CLÉ D'ACCÈS ci-dessus.
Rôles	Identifiant externe	Il s'agit d'un identifiant unique généré automatiquement pour accorder l'accès aux ressources AWS. Il est utilisé par l'utilisateur pour ajouter une relation de confiance au rôle.
	ARN de l'utilisateur	Il s'agit d'un identifiant unique généré automatiquement attribué à un IAM. Il est utilisé par l'utilisateur pour ajouter une relation de confiance au rôle.
	ARN	Un identifiant unique attribué à chaque ressource AWS.
	HTTP Proxy	(Facultatif) Serveur mandataire requis pour que Cisco Secure Workload atteigne AWS.

Nom du paramètre	Attribut	Description
	Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire d'AWS. La valeur par défaut et minimale est de 3 600 secondes.
	Delta Scan Interval	La fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles apportées aux données d'inventaire auprès d'AWS. La valeur par défaut et minimale est de 600 secondes.

Étape 12 Cliquez sur Next (suivant).

Étape 13 La page suivante affiche une **arborescence des ressources** que l'utilisateur peut développer pour visualiser différentes régions. À l'intérieur de la région, vous pouvez cocher ou décocher les cases des ressources pour obtenir la liste des VPC et des grappes EKS d'AWS.

Étape 14 Dans la liste des réseaux virtuels (VPC), choisissez les VPC pour lesquels vous souhaitez activer les fonctionnalités que vous avez sélectionnées.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

Notez que, comme EKS prend uniquement en charge la capacité de collecte d'étiquettes, aucune sélection de capacité explicite n'a été fournie. La sélection d'une grappe EKS activera implicitement la capacité prise en charge. Pour chaque grappe pour laquelle vous activez cette fonctionnalité, saisissez le **Assume Role ARN** (ARN du rôle assumé) (le numéro de ressource Amazon du rôle à assumer lors de la connexion à Cisco Secure Workload.

Enable Segmentation (activer la segmentation) sur les VPC supprimera le ou les groupes de sécurité existants et fournira un accès par défaut à tous les VPC.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Ultérieurement, lorsque vous serez prêt à appliquer la politique de segmentation pour des VPC spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces VPC. Consultez le document de Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.

Étape 15 Pour la grappe EKS, vous pouvez autoriser l'accès au rôle AWS IAM en fournissant l'ID d'accès Assume Role ARN pour vous connecter au connecteur AWS.

Étape 16 Une fois vos sélections terminées, cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation soit terminée.

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous activez l'acquisition de flux, cela prendre jusqu'à 25 minutes avant que les flux ne commencent à s'afficher dans la page **Investigate** > **Traffic** (Enquêter sur le trafic).

- (Facultatif) Pour approfondir les données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail basées sur VPC. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur AWS pour qu'il recueille les étiquettes et les flux d'acquisition, suivez le processus standard pour créer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier les portées (en général une pour chaque VPC); créer un espace de travail pour chaque portée; découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier que vos politiques respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un VPC particulier, revenez à la configuration du connecteur pour activer la segmentation pour le VPC. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, à la page 252.

Si vous avez activé l'option des services gérés par Kubernetes (EKS) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez la section *Agents Kubernetes/OpenShift : Visibilité et application approfondies* dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur AWS

Vous pouvez modifier un connecteur AWS, par exemple pour activer l'application de la segmentation pour des VPC spécifiques ou pour apporter d'autres modifications.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procedure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage (Gestion)** > **Workloads(Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **AWS**.

Étape 3 Si vous possédez plusieurs connecteurs AWS, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, consultez Configurer un nouveau connecteur AWS , on page 247.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données EKS), vous devez télécharger le modèle Cloud Formation (CFT) révisé et le téléverser sur AWS avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez satisfait aux conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de

segmentation pour l'inventaire AWS. Sur la page qui répertorie les VPC, choisissez **Enable Segmentation** (activer la segmentation) pour les VPC sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des VPC sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this step** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser) > Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portée pour les VPC sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parentale au-dessus de l'arborescence des portées, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS

Warning Avant d'activer l'application de la segmentation sur un VPC, créez une sauvegarde des groupes de sécurité sur ce VPC. L'activation de la segmentation pour un VPC supprime les groupes de sécurité existants de ce VPC. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité.

Lors de la création de politiques :

- Comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.
- Étant donné qu'AWS n'autorise que les règles ALLLOW (Autoriser) dans les groupes de sécurité, vos politiques de segmentation ne doivent inclure que des politiques Allow, sauf la politique collectrice Catch-All, qui doit avoir l'action Deny (Refuser).

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le VPC associé. Si vous activez la segmentation pour un VPC qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce VPC.

Lorsque vous êtes prêt à appliquer une politique pour un VPC, modifiez le connecteur AWS (voir Modifier un connecteur AWS) et activez la segmentation pour ce VPC.

Afficher les étiquettes d'inventaire, les détails et l'état d'application AWS

Pour afficher des informations résumées sur un connecteur AWS, accédez à la page du connecteur (Manage > Connectors), (Gérer > Connecteurs) puis sélectionnez le connecteur en haut de la page. Pour plus de détails, cliquez sur la ligne d'un VPC.

Pour afficher des informations sur l'inventaire de VPC AWS, cliquez sur une adresse IP dans la page AWS Connectors (Connecteurs AWS) afin d'afficher la page Inventory Profile (Profil d'inventaire) pour cette charge de travail. Pour en savoir plus sur les profils d'inventaire, consultez Profil d'inventaire.

Pour en savoir plus sur les étiquettes, consultez :

- Étiquettes générées par les connecteurs infonuagiques

- Étiquettes liées aux grappes Kubernetes

Des politiques concrètes pour l'inventaire VPC sont générées en fonction de leur valeur d'étiquette orchestrator_system/interface_id. Vous pouvez le voir sur la page Inventory Profile (Profil d'inventaire).

Pour afficher l'état d'application, choisissez **Defend (Défendre)** > **Enforcement Status ('État d'application)** dans la barre de navigation à gauche de la fenêtre Cisco Secure Workload. Pour en savoir plus, consultez État d'application pour les connecteurs du nuage.

Résoudre les problèmes de connecteur AWS

Problème : La page Enforcement Status (État de la mise en application) indique qu'une politique concrète a été SKIPPED (IGNORÉE).

Solution : Cette situation se produit lorsque le nombre de groupes de sécurité dépasse les limites d'AWS, telles que configurées dans le connecteur AWS.

Lorsqu'une politique concrète s'affiche comme SKIPPED (IGNORÉE), les nouveaux groupes de sécurité ne sont pas mis en œuvre et les groupes de sécurité existants sur AWS restent en vigueur.

Pour résoudre ce problème, voyez si vous pouvez consolider les politiques, par exemple en utilisant un sous-réseau plus grand dans une politique plutôt que plusieurs avec des sous-réseaux plus petits.

Si vous choisissez d'augmenter les limites du nombre de règles, vous devez communiquer avec Amazon avant de modifier les limites dans la configuration du connecteur AWS.

Contexte :

Des politiques concrètes sont générées pour chaque VPC lorsque la segmentation est activée. Ces politiques concrètes sont utilisées pour créer des groupes de sécurité dans AWS. Cependant, AWS et Cisco Secure Workload comptabilisent les politiques différemment. Lors de la conversion des politiques Cisco Secure Workload en groupes de sécurité AWS, AWS compte chaque sous-réseau unique comme une règle.

Exemple de comptabilisation :

Examinez l'exemple de politique Cisco Secure Workload suivant :

SORTANT : ensemble d'adresses du client -> ensemble d'adresses du fournisseur – Autoriser les ports TCP 80, 8080

AWS compte cette politique comme (le nombre de sous-réseaux uniques dans l'ensemble d'adresses du fournisseur) multiplié par (le nombre de ports uniques).

Ainsi, si l'ensemble d'adresses du fournisseur se compose de 20 sous-réseaux uniques, cette politique Cisco Secure Workload unique compte dans AWS comme 20 (sous-réseaux uniques) * 2 (ports uniques) = 40 règles dans les groupes de sécurité.

Gardez à l'esprit que, comme les VPC sont dynamiques, le nombre de règles l'est également : les nombres sont donc approximatifs.

Problème : AWS autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes s'exécutant sur AWS (EKS)

Si vous avez déployé Amazon Elastic Kubernetes Service (EKS) sur votre nuage AWS, vous pouvez utiliser un connecteur AWS pour extraire l'inventaire et les étiquettes (balises EKS) de votre grappe Kubernetes.

Lorsqu'un connecteur AWS est configuré pour extraire des métadonnées de services Kubernetes gérés, Cisco Secure Workload se connecte au serveur d'API de la grappe et suit l'état des nœuds, des pods et des services de cette grappe. Pour les étiquettes Kubernetes collectées et générées à l'aide de ce connecteur, consultez Étiquettes liées aux grappes Kubernetes.

Exigences et prérequis EKS

- Vérifiez que votre version de Kubernetes est prise en charge. Consultez https://www.cisco.com/go/secure-workload/requirements/integrations.
- Configurer l'accès requis dans EKS, comme décrit ci-dessous.

Rôles et privilèges d'accès EKS

Les informations d'identification de l'utilisateur et l'ARN AssumeRole (le cas échéant) doivent être configurées avec un ensemble minimal de privilèges. L'utilisateur/le rôle doit être spécifié dans la carte de configuration aws-auth.yaml. La carte de configuration aws-auth.yaml peut être modifiée à l'aide de la commande suivante.

```
$ kubectl edit configmap -n kube-system aws-auth
```

Si AssumeRole n'est pas utilisé, l'utilisateur doit être ajouté à la section « mapUsers » de la carte de configuration aws-auth.yaml avec le groupe approprié. Si l'ARN AssumeRole est spécifié, le rôle doit être ajouté à la section « mapRoles » de la carte de configuration aws-auth.yaml. Un exemple de carte de configuration aws-auth.yaml avec AssumeRole est fourni ci-dessous.

```
apiVersion: v1
data:
  mapAccounts: |
    []
  mapRoles: |
    - "groups":
      - "system:bootstrappers"
      - "system:nodes"
     "rolearn": "arn:aws:iam::938996165657:role/eks-cluster-20210114181445234700000000a"

      "username": "system:node:{{EC2PrivateDNSName}}"
    - "rolearn": arn:aws:iam::938996165657:role/BasicPrivilegesRole
      "username": secure.workload.read.only-user
      "groups":
        - secure.workload.read.only

  mapUsers: |
    []
kind: ConfigMap
metadata:
  creationTimestamp: "2021-01-14T18:14:47Z"
  managedFields:
  - apiVersion: v1
    fieldsType: FieldsV1
    fieldsV1:
      f:data:
        .: {}
        f:mapAccounts: {}
        f:mapRoles: {}
        f:mapUsers: {}
    manager: HashiCorp
    operation: Update
    time: "2021-01-14T18:14:47Z"
  name: aws-auth
  namespace: kube-system
```

```
    resourceVersion: "829"
    selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
    uid: 6c5a3ac7-58c7-4c57-a9c9-cad701110569
```

Considérations RBAC spécifiques à EKS

Créer un lien de rôle de grappe entre le rôle de grappe et le compte d'utilisateur/de service.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: csw-clusterrolebinging
subjects:
- kind: User
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
  kubectl create -f clusterrolebinding.yaml
clusterrolebinding.rbac.authorization.k8s.io/csw-clusterrolebinging created
```

Pour en savoir plus sur les rôles et l’accès EKS, consultez la section Rôles EKS et privilèges d’accès.

Configurer les paramètres EKS dans l'assistant du connecteur AWS

Vous activez la fonctionnalité des Services gérés Kubernetes lorsque vous configurez le connecteur AWS. Consultez la section Configurer un nouveau connecteur AWS , on page 247.

Vous aurez besoin de l'ARN Assume Role (ARN Assumer le rôle) pour chaque grappe EKS. Pour en savoir plus, consultez https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html.

Si vous utilisez l’utilisateur AWS pour accéder à la grappe EKS, permettez à l’utilisateur d’accéder à la fonction Assumer le rôle.

Si vous utilisez un rôle IAM entre comptes, permettez au rôle IAM d’accéder à Assumer le rôle.

Prise en charge de l’équilibreur de charge EKS

Nous ajoutons la prise en charge des services de l’équilibreur de charge dans EKS. Les agents Cisco CSW appliquent les règles aux hôtes consommateurs et aux hôtes/pods fournisseurs.

Un équilibreur de charge EKS offre deux options :

1. Conserver l’adresse IP du client.
2. Sur le pod du fournisseur, nous générons
3. Type de cible.

Avant de commencer les scénarios, pour l’intent de politique suivante :

Le service de consommateur à fournisseur, de protocole de service et de port avec des règles d’action Allow (autorisation) pour divers cas est généré comme suit :

Scénario	Conserver l'adresse IP du client	Type de cible
1	Activé	IP
2	Activé	Instance

Scénario	Conserver l'adresse IP du client	Type de cible
3	Désactivé	IP
4	Désactivé	Instance

Cas 1 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Il n'y a pas de règle d'hôte sur le nœud fournisseur, mais nous générons une règle d'entrée sur le pod fournisseur avec la source comme pod consommateur, la destination comme pod de fournisseur (tout), le protocole comme protocole cible, le port comme port cible, et (Allow, autoriser) comme action.

Cas 2 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Le nœud fournisseur génère une règle de préroutage dont la source est le consommateur et la destination tous les nœuds fournisseurs, le protocole le protocole du service, le port le port du nœud du service et l'action l'autorisation.

Sur le pod fournisseur, nous générons une règle d'entrée dont la source est le nœud fournisseur, la destination le pod fournisseur (quelconque), le protocole le protocole cible, le port le port cible et l'action l'autorisation.

Cas 3 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Il n'y a aucune règle d'hôte sur le nœud du fournisseur. Sur le pod fournisseur, nous générons une règle d'entrée avec la source comme ip d'entrée lb, la destination comme pod fournisseur (quelconque), le protocole comme protocole cible, le port comme port cible et l'action comme autorisation.

Cas 4 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Le nœud fournisseur génère une règle de préroutage qui définit les adresses IP d'entrée comme source et tous les nœuds fournisseurs comme destination. La règle spécifie le protocole du service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod fournisseur, nous générons une règle d'entrée dont la source est le nœud fournisseur, la destination le pod fournisseur (quelconque), le protocole le protocole cible, le port le port cible et l'action l'autorisation.

Connecteur Azure

Le connecteur Azure se connecte à votre compte Microsoft Azure pour effectuer les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses balises) en direct à partir de vos réseaux virtuels Azure (VNets)** Azure vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload peut intégrer les balises associées aux machines virtuelles et aux interfaces réseau, qui peuvent ensuite être utilisées comme étiquettes dans Cisco Secure Workload pour la visualisation des données d'inventaire et des flux de trafic et les définitions de politiques. Ces métadonnées sont synchronisées en permanence.

Les balises des charges de travail et des interfaces réseau de l'abonnement associé au connecteur sont intégrées. Si les charges de travail et les interfaces réseau sont configurées, les balises sont fusionnées et affichées dans Cisco Secure Workload. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques, à la page 352.

- **Acquisition des journaux de flux** Le connecteur peut intégrer les journaux de flux que vous configurez dans Azure pour vos groupes de sécurité réseau (NSG). Vous pouvez ensuite utiliser ces données de télémétrie dans Cisco Secure Workload pour la génération de politiques de visualisation et de segmentation.
- **Segmentation** Lorsque l'application de la politique de segmentation est activée pour un réseau virtuel, les politiques Cisco Secure Workload sont appliquées à l'aide des groupes de sécurité réseau natifs d'Azure.
- **Acquisition automatisée des métadonnées des grappes AKS** Lorsque les services Azure Kubernetes (AKS) sont exécutés sur Azure, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et d'espaces liées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir laquelle des capacités ci-dessus vous souhaitez activer pour chaque réseau virtuel.

Le connecteur Azure prend en charge plusieurs abonnements.

Remarque Les régions de la Chine ne sont actuellement pas prises en charge.

Exigences et prérequis Azure

Pour toutes les fonctionnalités : un seul connecteur peut gérer plusieurs abonnements. Vous aurez besoin d'un ID d'abonnement pour configurer le connecteur. Cet ID d'abonnement peut être l'un des nombreux ID d'abonnement qui sont intégrés à un connecteur.

Dans Azure, créer et enregistrer une application à l'aide d'Azure Active Directory (AD). Vous aurez besoin des renseignements suivants provenant de cette application :

- ID (client) d'application
- ID de l'annuaire (détenteur)
- Renseignements d'authentification client (vous pouvez utiliser un certificat ou une clé secrète client)
- Identifiant d'abonnement

L'assistant de configuration du connecteur génère un modèle de gestionnaire de ressources Azure (ARM) que vous pouvez utiliser pour créer un rôle personnalisé avec les autorisations nécessaires pour les fonctionnalités du connecteur que vous choisissez d'activer. Ces autorisations s'appliqueront à toutes les ressources de l'abonnement que vous spécifiez pour le connecteur. Assurez-vous que vous disposez des autorisations dans Azure pour charger ce modèle.

Si la connectivité l'exige, assurez-vous qu'un serveur mandataire HTTP est disponible pour cette intégration.

Chaque réseau virtuel (VNet) ne peut appartenir qu'à un seul connecteur Azure. Un compte Azure peut avoir plusieurs connecteurs Azure.

Ce connecteur ne nécessite pas d'appliance virtuelle.

Pour la collecte d'étiquettes et de l'inventaire : aucune condition préalable supplémentaire n'est requise.

Pour l'acquisition des journaux de flux : chaque réseau virtuel (VNet) doit avoir au moins un sous-réseau configuré.

Chaque sous-réseau de chaque réseau virtuel doit être associé à un groupe de sécurité réseau (NSG). Vous pouvez associer un seul NSG à plusieurs sous-réseaux. Vous pouvez définir n'importe quel groupe de ressources lors de la configuration du groupe de sécurité réseau.

Seul le trafic qui atteint une règle NSG sera inclus dans les journaux de flux. Par conséquent, chaque groupe de sécurité réseau devrait avoir au moins une règle pour le trafic entrant et une règle pour le trafic sortant qui s'applique à n'importe quelle source et à toute destination. L'équivalent d'une règle collectrice globale dans Cisco Secure Workload. (Par défaut, les groupes de sécurité réseau incluent ces règles).

Les journaux de flux doivent être activés pour chaque groupe de sécurité réseau.

- Un compte de stockage dans Azure est requis. Des autorisations d'accès doivent être incluses pour l'abonnement que vous utilisez pour ce connecteur.
- Les journaux de flux doivent utiliser la version 2.
- La durée de conservation peut être de deux jours (le connecteur extrait de nouvelles données de flux toutes les minutes, et deux jours devraient laisser suffisamment de temps pour résoudre les échecs de connexion).

Pour la segmentation : l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Lorsque vous activez la segmentation pour un réseau virtuel (VNet), toutes les règles existantes sont supprimées des groupes de sécurité réseau associés aux sous-réseaux et aux interfaces réseau qui font partie de ces sous-réseaux. Sauvegardez vos règles existantes de groupe de sécurité réseau du sous-réseau et de l'interface réseau avant d'activer la segmentation dans le connecteur.

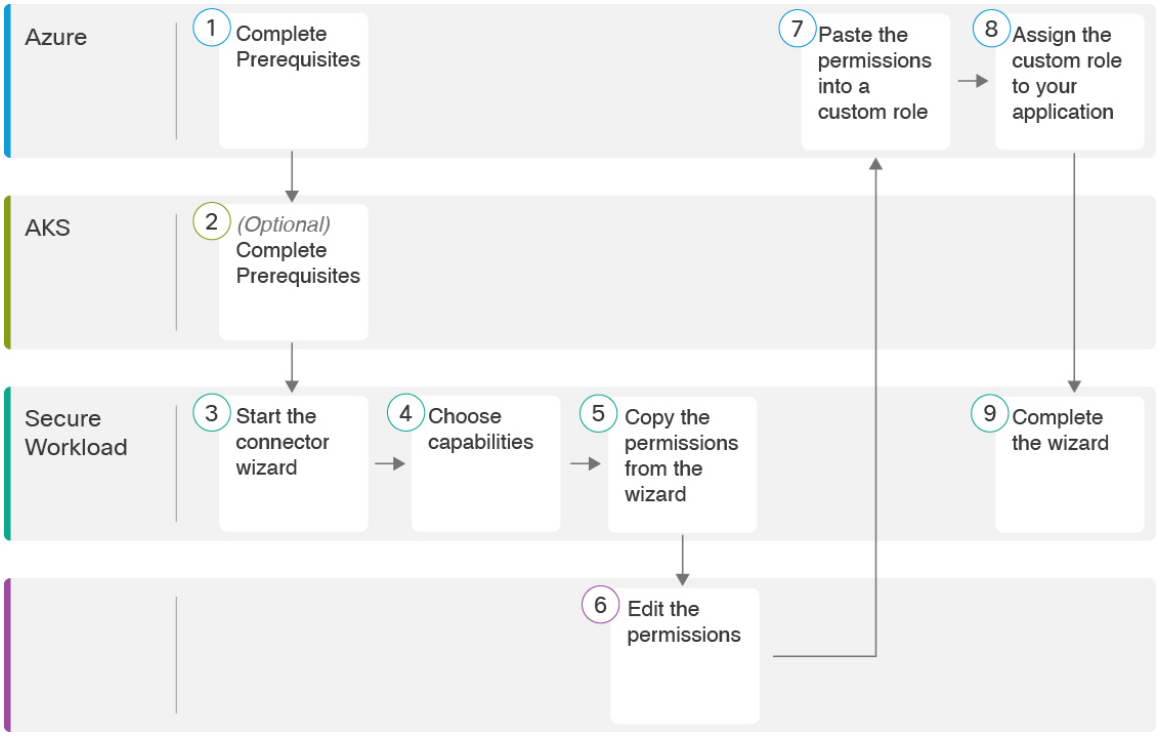
Voir également Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 263, ci-dessous.

Pour les services Kubernetes gérés (AKS) : si vous activez l'option Kubernetes AKS, consultez les exigences et les conditions préalables dans la section des services Kubernetes gérés fonctionnant sur Azure (AKS) ci-dessous, .

Présentation de la configuration du connecteur Azure

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour en savoir plus sur les renseignements importants, consultez la rubrique suivante (Configurer un connecteur Azure).

Illustration 101 : Présentation de la configuration du connecteur Azure



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un connecteur Azure

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur le connecteur Azure.

Étape 3 Cliquez sur **Enable** (activer) pour le premier connecteur (dans une portée racine) ou **Enable Another** (activer un autre connecteur) pour les connecteurs supplémentaires de la même portée racine.

Étape 4 Comprenez et respectez les exigences et les prérequis dans le document Exigences et prérequis Azure, puis cliquez sur Get Started (Démarrer).

Étape 5 Nommez le connecteur et choisissez les fonctionnalités souhaitées :

Les sélections que vous effectuez sur cette page sont utilisées uniquement pour déterminer les privilèges inclus dans le modèle de gestionnaire de ressources Azure (ARM) qui sera généré à l'étape suivante et pour afficher les paramètres que vous devrez configurer.

Pour activer la segmentation, vous devez également activer **Gather Labels** (Regrouper les étiquettes).

L'activation de la segmentation sur cette page ne permet pas en elle-même l'application des politiques et n'affecte pas les groupes de sécurité réseau existants. L'application des politiques et la suppression des groupes de sécurité existants se produisent uniquement si vous activez la segmentation pour les réseaux virtuels ultérieurement dans l'assistant. Vous pouvez revenir à cet assistant plus tard pour activer l'application de la politique de segmentation pour les réseaux virtuels individuels.

Étape 6 Cliquez sur **Next** (suivant) et lisez les informations sur la page de configuration.

Étape 7 Votre abonnement doit disposer des privilèges requis pour que vous puissiez passer à la page suivante de l'assistant.

Pour utiliser le modèle Azure Resource Manager (ARM) fourni pour attribuer les autorisations requises pour le connecteur :

1. Téléchargez le modèle ARM à partir de l'assistant.
2. Modifiez le texte du modèle pour remplacer **<subscription_ID>** par votre numéro d'abonnement.

   Remarque Pour un connecteur, vous pouvez créer plusieurs ID d'abonnement dans le compte Azure.

   Vous pouvez saisir plusieurs ID d'abonnement lorsque les informations d'authentification appartiennent au même ID d'abonnement.

3. Dans Azure, créez un rôle personnalisé dans l'abonnement applicable.
4. Dans le formulaire de rôle personnalisé, pour les autorisations de référence, choisissez **Start from zero** (Démarrer à partir de zéro).
5. Dans l'onglet JSON du formulaire de création de rôle personnalisé, collez le texte du fichier modifié que vous avez téléchargé à partir de l'assistant de connecteur.
6. Enregistrez le rôle personnalisé.
7. Associez le rôle personnalisé à l'application que vous avez configurée dans les conditions préalables pour cette procédure.

Ce modèle dispose des autorisations IAM requises pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option des services gérés par Kubernetes, vous devez configurer séparément les autorisations pour AKS. Consultez Services gérés Kubernetes fonctionnant sur Azure (AKS), à la page 264.

Étape 8 Configurer les paramètres :

Attribut	Description
SubscriptionID	ID de l'abonnement Azure que vous associez à ce connecteur.
ClientID	**ID d'application (client)** de l'application que vous avez créée dans Azure pour ce connecteur.
TenantID	L' **ID de l'annuaire (détenteur)** de l'application que vous avez créée dans Azure pour ce connecteur.
Clé secrète du client ou certificat du client	Pour l'authentification, vous pouvez utiliser une clé secrète client ou un certificat client et une clé. Obtenez l'un ou l'autre à partir du lien **Informations d'identification client** dans l'application que vous avez créée dans Azure pour ce connecteur. Si vous utilisez un certificat : le certificat doit être non chiffré. Seuls les certificats RSA sont pris en charge Les clés privées peuvent être PKCS1 ou PKCS8.

Attribut	Description
HTTP Proxy	Serveur mandataire requis pour que Cisco Secure Workload atteigne Azure. Ports serveur mandataire pris en charge : 80, 8080, 443 et 3128.
Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire d'Azure. La valeur par défaut et minimale est de 3 600 secondes.
Delta Scan Interval	Fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles des données d'inventaire auprès d'Azure. La valeur par défaut et minimale est de 600 secondes.

Étape 9 Cliquez sur **Next** (suivant). Le système peut nécessiter quelques minutes pour obtenir la liste des réseaux virtuels et des grappes AKS d'Azure.

Étape 10 Dans la liste des réseaux virtuels et des grappes AKS pour chaque réseau virtuel, choisissez les réseaux virtuels et les grappes AKS pour lesquels vous voulez activer les fonctionnalités sélectionnées.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

Notez que, puisqu'AKS prend uniquement en charge la capacité de collecte d'étiquettes, aucune sélection de capacité explicite n'a été fournie. La sélection d'une grappe AKS activera implicitement la capacité prise en charge. Téléversez le certificat client et la clé pour chaque grappe pour laquelle vous activez cette fonctionnalité.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Plus tard, lorsque vous serez prêt à appliquer la politique de segmentation pour des réseaux virtuels spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces réseaux. Consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 263.

Étape 11 Une fois vos sélections terminées, cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation soit terminée.

La page View Groups (Afficher les groupes) affiche tous les réseaux virtuels que vous avez activés pour les fonctionnalités de la page précédente, regroupés par région. Chaque région et chaque réseau virtuel dans chaque région constitue une nouvelle portée.

Étape 12 (Facultatif) Choisissez la portée parente sous laquelle ajouter le nouvel ensemble de portées. Si vous n'avez encore défini aucune portée, votre seule possibilité est la portée par défaut.

Étape 13 (Facultatif) Pour accepter tous les paramètres configurés dans l'assistant, *y compris* l'arborescence de portée hiérarchique, cliquez sur **Save**(enregistrer) .

Pour accepter tous les paramètres à l'*exception* de l'arborescence de la portée hiérarchique, cliquez sur **Skip** (Ignorer) cette étape.

Vous pourrez créer ou modifier manuellement l'arborescence de la porte ultérieurement, sous **Organiser (Organiser)** > **Scopes and Inventory (Portées et inventaires**).

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous avez activé l'acquisition de flux, 25 minutes peuvent être nécessaires avant que les flux ne commencent à s'afficher sur la page **Investigate (Enquêter)** > **Traffic (Trafic)** .
- (Facultatif) Pour approfondir des données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail de réseau virtuel. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur Azure pour recueillir des étiquettes et des flux d'acquisition, suivez le processus standard pour créer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier la portée (en général une pour chaque réseau virtuel); créer un espace de travail pour chaque portée; découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier qu'elles respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un réseau virtuel donné, revenez à la configuration du connecteur pour activer la segmentation pour ce réseau virtuel. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 263.

Si vous avez activé l'option des services gérés par Kubernetes (AKS) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez Installer les agents Kubernetes ou OpenShift pour une visibilité et une application approfondies, à la page 42 dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur Azure

Vous pouvez modifier un connecteur Azure, par exemple pour activer l'application de la segmentation pour des réseaux virtuels spécifiques ou pour apporter d'autres modifications.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur **Azure**.

Étape 3 Si vous avez plusieurs connecteurs Azure, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, reportez-vous à Configurer un connecteur Azure, à la page 259.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données AKS), vous devez télécharger le modèle ARM révisé, modifier le texte du nouveau modèle pour préciser l'ID d'abonnement, et charger le nouveau modèle dans le rôle personnalisé que vous voulez. créé dans Azure avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez rempli les conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 263. Ensuite, sur la page de l'assistant qui répertorie les réseaux virtuels, choisissez **Enable Segmentation** (activer la segmentation) pour les réseaux virtuels sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des réseaux virtuels sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this étape** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser) > Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portées pour les réseaux virtuels sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parente dans la partie supérieure de l'arborescence, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure

Avertissement Avant d'activer l'application de la segmentation sur un réseau virtuel, créez une sauvegarde des groupes de sécurité réseau sur ce réseau virtuel. L'activation de la segmentation pour un réseau virtuel supprime les règles existantes du groupe de sécurité réseau associé à ce dernier. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité réseau.

Lors de la création de politiques : comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le réseau virtuel associé. Si vous activez la segmentation pour un réseau virtuel qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce réseau virtuel.

Lorsque vous êtes prêt à appliquer la politique pour un réseau virtuel, modifiez le connecteur Azure (voir Modifier un connecteur Azure, à la page 262) et activez la segmentation pour ce réseau virtuel.

Notez que si un sous-réseau n'est associé à aucun groupe de sécurité de réseau, Cisco Secure Workload n'applique pas la politique de segmentation sur ce sous-réseau. Lorsque vous appliquez la politique de segmentation sur un réseau virtuel, le groupe de sécurité réseau au niveau du sous-réseau est modifié pour autoriser tout le trafic, et les politiques Cisco Secure Workload remplacent le groupe de sécurité réseau au niveau de l'interface. Un groupe de sécurité réseau pour l'interface est automatiquement créé s'il n'est pas déjà présent.

Afficher les étiquettes d'inventaire, les détails et l'état d'application d'Azure

Pour afficher des renseignements résumés sur un connecteur Azure, accédez à la page du connecteur (Manage > Connectors) (Gérer > Connecteurs), puis sélectionnez le connecteur en haut de la page. Pour plus de détails, cliquez sur une ligne VNet.

Pour afficher des informations sur l'inventaire VNet Azure, cliquez sur une adresse IP dans la page Azure Connectors (connecteurs Azure) afin d'afficher la page Inventory Profile (Profil d'inventaire) pour cette charge de travail. Pour en savoir plus sur les profils d'inventaire, consultez Profil d'inventaire.

Pour en savoir plus sur les étiquettes, consultez :

- Étiquettes générées par les connecteurs infonuagiques
- Étiquettes liées aux grappes Kubernetes

Des politiques concrètes pour l'inventaire de réseau virtuel sont générées en fonction de leur valeur d'étiquette orchestrator_system/interface_id. Vous pouvez le voir sur la page Inventory Profile (Profil d'inventaire).

Pour afficher l'état d'application, choisissez **Defend (Défendre)** > **Enforcement Status ('État d'application)** dans la barre de navigation à gauche de la fenêtre Cisco Secure Workload. Pour en savoir plus, consultez État d'application pour les connecteurs du nuage.

Résoudre les problèmes de connecteur Azure

Problème : Azure autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes fonctionnant sur Azure (AKS)

Si vous avez déployé Azure Kubernetes Services (AKS) sur votre nuage Azure, vous pouvez utiliser un connecteur Azure pour extraire dynamiquement l'inventaire et les étiquettes (balises AKS) de votre grappe Kubernetes.

Lorsqu'un connecteur Azure est configuré pour extraire des métadonnées de services Kubernetes gérés, Cisco Secure Workload suit l'état des nœuds, des pods et des services de cette grappe.

Pour les étiquettes Kubernetes collectées et générées à l'aide de ce connecteur, consultez Étiquettes liées aux grappes Kubernetes.

Requirements and Prerequisites for AKS

- Verify that your Kubernetes version is supported. See the Compatibility Matrix for the operating systems, external systems, and connectors for Secure Workload agents.
- Enable and configure the Managed Kubernetes Services (AKS) capability when you configure the Azure connector. See Configurer un connecteur Azure for details.

Prise en charge de l'équilibreur de charge AKS

AKS prend en charge la conservation de l'adresse IP du client.

Pour l'intent de politique suivant :

Le service de consommateur à fournisseur, le protocole de service et le port avec des règles d'action Allow (autorisation) dans différents scénarios se génèrent comme suit :

Scénario	Conserver l'adresse IP du client
1	Activé
2	Désactivé

Scénario 1 : la fonction Conserver l'adresse IP du client est **activée**.

Sur le nœud du consommateur, nous générons une règle de sortie avec le service du consommateur vers l'équilibreur de charge (lb ingress ip), le protocole du service et le port sont autorisés.

Une règle de préroutage générée pour le nœud fournisseur, qui définit le consommateur comme source et tous les nœuds fournisseurs comme destination. La règle inclut le protocole de service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod du fournisseur, nous générons une règle d'entrée avec source comme nœuds de fournisseur, une destination comme pod de fournisseur (n'importe lequel), le protocole comme protocole cible, le port comme port cible et l'action comme allow (autoriser).

Scénario 2 : la fonction de conservation de l'adresse IP du client est **désactivée**.

Sur le nœud du consommateur, nous générons une règle de sortie avec le service du consommateur vers l'équilibreur de charge (lb ingress ip), le protocole du service et le port sont autorisés.

Le nœud fournisseur génère une règle de préroutage qui définit les adresses IP d'entrée comme source et tous les nœuds fournisseurs comme destination. La règle spécifie le protocole du service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod du fournisseur, nous générons une règle d'entrée avec la source comme nœuds de fournisseur, la destination comme pod de fournisseur (n'importe quel), le protocole comme protocole cible, le port comme port cible et l'action comme allow (autoriser).

Connecteur GCP

Le connecteur Google Cloud Platform se connecte à GCP pour effectuer les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses balises) en direct à partir du nuage privé virtuel (VPC) GCP**

  GCP vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload interrogera les balises de ces ressources, qui peuvent ensuite être utilisées pour la visualisation des données d'inventaire et des flux de trafic, et pour la définition de politiques. Cette fonctionnalité maintient le mappage des balises de ressources à jour en synchronisant constamment ces données.

  Les balises des charges de travail et des interfaces réseau d'un VPC GCP sont intégrées. Si les charges de travail et les interfaces réseau sont configurées, les balises sont fusionnées et affichées dans Cisco Secure Workload. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques, à la page 352.

- **Acquisition des journaux de flux du VPC** si vous avez configuré les journaux de flux VPC dans GCP à des fins de surveillance, Cisco Secure Workload peut procéder à l'acquisition des informations des journaux de flux en lisant le compartiment de stockage Google correspondant. Ces données de télémétrie peuvent être utilisées pour la génération de politiques de visualisation et de segmentation.

- **Segmentation** : l'activation de cette option permettra à Cisco Secure Workload de programmer les politiques de sécurité à l'aide du pare-feu VPC natif de GCP. Lorsque l'application est activée pour un VPC, les politiques pertinentes sont automatiquement programmées sur le pare-feu de celui-ci.

- **Acquisition automatisée des métadonnées des grappes GKE** (capacités K8s) lorsque Google Kubernetes Engine (GKE) s'exécute sur GCP, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et de pods associées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir laquelle des capacités ci-dessus vous souhaitez activer pour chaque VPC.

Exigences et conditions préalables des connecteurs GCP

Pour toutes les fonctionnalités : créez un compte de service dédié dans GCP ou identifiez un compte de service GCP existant pour ce connecteur. L'assistant de configuration du connecteur génère une liste de politiques IAM que vous pouvez utiliser pour attribuer les privilèges requis à ce compte de service. Assurez-vous que vous avez les autorisations dans GCP pour charger cette liste de politiques IAM.

Remarque La méthode recommandée pour appliquer l'autorisation de la liste de politiques IAM au compte de service consiste à utiliser la CLI.

Chaque VPC ne peut appartenir qu'à un seul connecteur GCP. Une grappe Cisco Secure Workload peut avoir plusieurs connecteurs GCP. Recueillez les informations décrites dans les tableaux Configurer un connecteur GCP, à la page 268, ci-dessous.

Ce connecteur ne nécessite pas d'appliance virtuelle.

- **Pour la collecte d'étiquettes et de l'inventaire :** aucune condition préalable supplémentaire n'est requise.
- **Pour l'acquisition des journaux de flux :** des définitions de journaux de flux au niveau VPC sont requises pour déclencher la collecte des journaux de flux.

  Pour utiliser l'acquisition des journaux de flux, l'utilisateur doit activer les journaux de flux sur les VPC souhaités et configurer un récepteur de routeur de journaux.

  Filtre d'inclusion pour le récepteur du routeur de journal :

  1. `resource.type="gce-subnetwork"`
  2. `log_name="projects/<project_id>/logs/compute.googleapis.com%2Fvpc_flows"`

  Choisissez la destination du récepteur en tant que compartiment de stockage infonuagique, puis choisissez l'ensemble de stockage souhaité.

  Lors de la configuration du connecteur GCP avec les journaux de flux d'entrée, il est obligatoire de saisir le nom du compartiment de stockage.

  Seuls les journaux de flux du VPC peuvent être intégrés.

  Les journaux de flux doivent être publiés dans le compartiment de stockage Google; Cisco Secure Workload ne peut pas collecter les données de flux de Google Cloud Operations Suite.

  Cisco Secure Workload peut acquérir des logs de flux à partir d'un compartiment de stockage Google associé à n'importe quel compte, si le compte utilisateur GCP fourni lors de la création du connecteur a accès à la fois aux journaux de flux VPC et au compartiment de stockage Google.

  Les attributs de journal de flux suivants (dans n'importe quel ordre) sont requis dans ce dernier : adresse source, adresse de destination, port source, port de destination, protocole, paquets, octets, heure de début, heure de fin, action, indicateurs TCP, ID d'interface, État du journal et direction du flux. Tout autre attribut est ignoré.

  Les journaux de flux doivent saisir le trafic autorisé et refusé.

- **Pour la segmentation :** l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Sauvegardez vos groupes de sécurité existants avant d'activer la segmentation dans le connecteur, car toutes les règles existantes seront remplacées lorsque vous activerez l'application de la politique de segmentation pour un VPC.

Voir également Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 272, ci-dessous.

- **Pour les services Kubernetes gérés (GKE) :** si vous activez l'option Kubernetes, consultez les exigences et les conditions préalables dans la section Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 273 ci-dessous, y compris les privilèges d'accès requis.

Configurer l'accès à plusieurs projets dans GCP

Pour configurer l'accès entre plusieurs projets dans GCP, vous pouvez suivre ces étapes :

Procédure

Étape 1 Connectez-vous à votre console GCP.

Étape 2 Cliquez sur le menu déroulant du projet dans la barre de navigation supérieure et sélectionnez **New Project** (Nouveau projet). Vous pouvez soit créer un nouveau projet, soit utiliser un projet existant avec le compte de service.

Étape 3 Saisissez un nom pour votre nouveau projet. Choisissez l'organisation à laquelle appartient le nouveau projet ou sélectionnez **No organization** (Aucune organisation) si vous n'en avez pas.

Étape 4 Cliquez sur le bouton **Create** (Créer) pour créer le nouveau projet.

Remarque Vous pouvez répéter les étapes 2 à 4 pour créer autant de projets que nécessaire.

Étape 5 Pour lier plusieurs projets à un seul compte de service, accédez à la page **IAM & Admin** et choisissez **Service Account** (Compte de service).

Étape 6 Cliquez sur le bouton **Create Service Account** (Créer un compte de service). Suivez les instructions pour créer le compte de service et lui accorder les autorisations nécessaires.

Remarque Vous pouvez soit utiliser un compte de service existant, soit créer un nouveau compte de service.

Étape 7 Sous l'onglet **Keys** (clés), cliquez sur **Add Key** (Ajouter une clé) pour générer une clé privée dans un fichier JSON.

Étape 8 Rendez-vous sur la page **IAM & Admin** de la console GCP et sélectionnez **IAM**.

Remarque Vous devez d'abord changer de projet avant de cliquer sur IAM & Admin, puis essayer d'accorder des privilèges.

Étape 9 Cliquez sur le bouton **Grant access** (accorder l'accès) pour ajouter un nouveau projet.

Étape 10 Dans le champ **New principals** (oNuveaux principaux), saisissez l'adresse courriel du compte de service que vous souhaitez associer au projet.

Étape 11 Cliquez sur le bouton **Save** (Enregistrer) pour associer le compte de service à votre projet.

Remarque Répétez ces étapes pour chaque projet que vous souhaitez lier à votre projet d'origine.

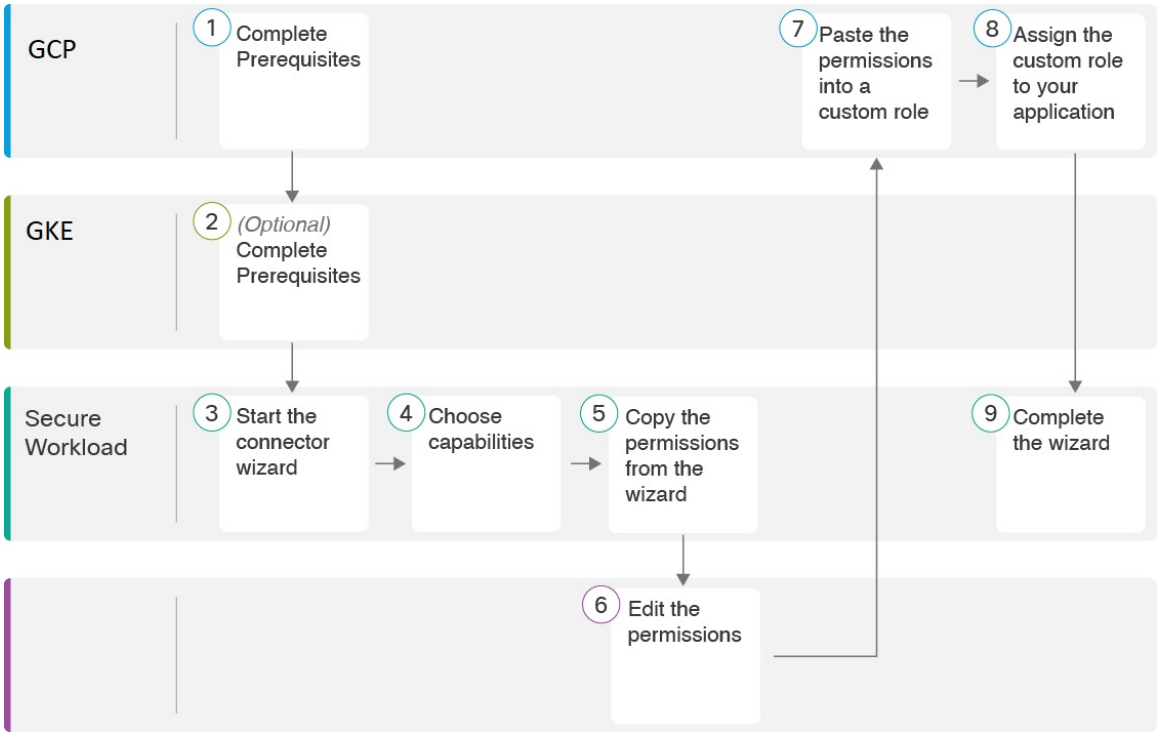
Vous pouvez gérer les autorisations du compte de service en vous rendant sur la page **IAM & Admin** de la console GCP et en sélectionnant **IAM** pour chaque projet.

Étape 12 Assurez-vous que le compte de service dispose d'autorisations pour le niveau de ressources ancêtre le moins élevé commun (ancêtre commun à tous les projets sélectionnés), tel qu'un dossier ou une organisation.

Aperçu de la configuration du connecteur GCP

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour en apprendre davantage, consultez la rubrique suivante (Configurer un connecteur GCP, à la page 268).

Illustration 102 : Aperçu de la configuration du connecteur GCP



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un connecteur GCP

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur le **GCP connector** (connecteur GCP).

Étape 3 Cliquez sur **Enable** (activer) pour le premier connecteur (dans une portée racine) ou **Enable Another** (activer un autre connecteur) pour les connecteurs supplémentaires de la même portée racine.

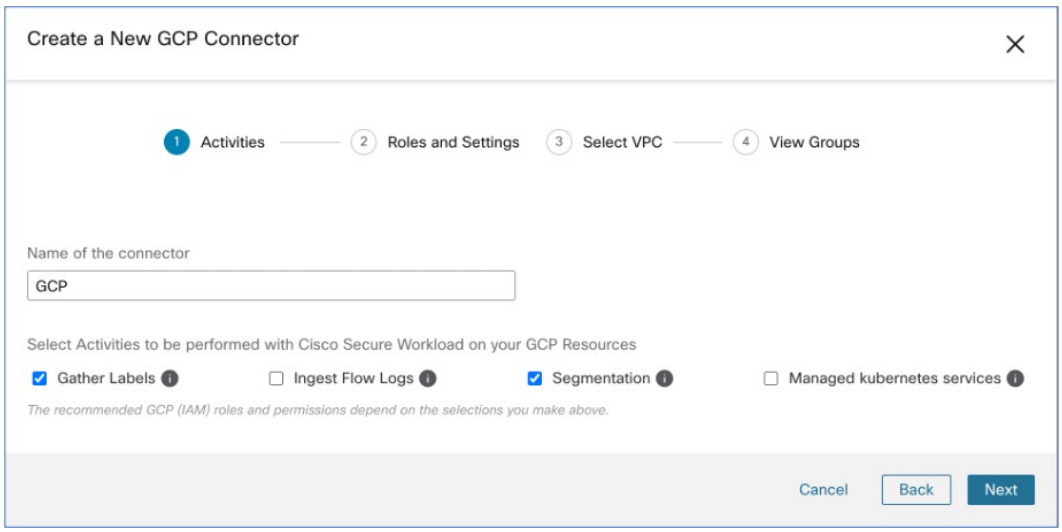
Étape 4 Comprenez et respectez les exigences et les conditions préalables indiquées dans Exigences et conditions préalables des connecteurs GCP, à la page 266 et Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 273, puis cliquez sur **Get Started** (Démarrer).

Étape 5 Attribuez un nom au connecteur et choisissez les fonctionnalités souhaitées, puis cliquez sur **Next** (Suivant).

Les sélections effectuées sur cette page servent uniquement à déterminer les privilèges inclus dans la liste de règles IAM qui sera générée à l'étape suivante, et à afficher les paramètres que vous devrez configurer.

Si la fonctionnalité **Injest Flow Logs** (injecter les journaux de flux) est cochée, vous devez saisir **le nom du compartiment de stockage des journaux** de flux à l'étape suivante.

Pour activer la **segmentation**, vous devez cocher **Gather Labels** (recueillir les étiquettes).



Étape 6 Téléchargez la liste des politiques de rôle personnalisé IAM générée.

Cette liste de politiques de rôles personnalisés IAM dispose des privilèges IAM requis pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option Kubernetes, vous devez configurer séparément les autorisations pour GKE.

Pour en savoir plus, consultez Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 273.

Étape 7 Chargez le fichier `json du compte de service` avec les fonctionnalités requises qui a été créé comme condition préalable.

Remarque Dans GCP, le connecteur unique prend en charge plusieurs projets et garantit que le compte de service est directement associé à tous les projets.

Étape 8 Saisissez le **nom de la compartiment de stockage des journaux de flux** si la fonctionnalité des journaux de flux d'entrée est cochée.

Étape 9 Configurez les paramètres suivants :

Attribut	Description
HTTP Proxy	serveur mandataire requis pour que Cisco Secure Workload atteigne GCP.
Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire de GCP. La valeur par défaut et minimale est de 3 600 secondes.

Attribut	Description
Delta Scan Interval	Fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles apportées aux données d'inventaire à partir de GCP. La valeur par défaut et minimale est de 600 secondes.

Étape 10 Cliquez sur **Next** (suivant). Quelques minutes peuvent être nécessaires pour que le système obtienne la liste des réseaux virtuels et des grappes GKE de votre (vos) projet(s) GCP.

Étape 11 Dans la liste des VPC (réseaux virtuels) et des grappes GKE, choisissez les ressources et leurs capacités respectives.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Ultérieurement, lorsque vous serez prêt à appliquer la politique de segmentation pour des VPC spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces VPC. Consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour un inventaire GCP.

Étape 12 Cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation se termine.

La page View Groups (Afficher les groupes) affiche tous les VPC que vous avez activés pour toutes les fonctionnalités sur la page précédente, regroupés par logic_group_id (CSW), qui est également un ID de projet (GCP). Chaque logic_group_id et chaque VPC de chaque logic_group_id est une nouvelle portée.

Étape 13 Choisissez la portée parente sous laquelle ajouter le nouvel ensemble de portées. Si vous n'avez encore défini aucune portée, votre seule possibilité est la portée par défaut.

Étape 14 Pour accepter tous les paramètres configurés dans l'assistant, *y compris* l'arborescence de portée hiérarchique, cliquez sur **Save**(enregistrer).

Pour accepter tous les paramètres à l'*exception* de l'arborescence de la portée hiérarchique, cliquez sur **Skip** (Ignorer) cette étape.

Vous pourrez créer ou modifier manuellement l'arborescence de la porte ultérieurement, sous **Organiser (Organiser)** > **Scopes and Inventory (Portées et inventaires**).

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous avez activé l'acquisition de flux, 25 minutes peuvent être nécessaires avant que les flux ne commencent à s'afficher sur la page **Investigate (Enquêter)** > **Traffic (Trafic)** .
- (Facultatif) Pour approfondir les données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail basées sur VPC. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur GCP pour recueillir des étiquettes et des flux d'acquisition, suivez le processus standard pour élaborer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier les portées (en général une pour chaque VPC); créer un espace de travail pour chaque portée;

découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier que vos politiques respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un VPC particulier, revenez à la configuration du connecteur pour activer la segmentation pour le VPC. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 272.

Si vous avez activé l'option des services gérés par Kubernetes (GKE) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez la section Installer les agents Kubernetes ou OpenShift pour une visibilité et une application approfondies dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur GCP

Si vous souhaitez activer la collecte de données à partir de grappes GKE ou de VPC différents ou supplémentaires, vous devrez peut-être charger un fichier json de compte de service avec les fonctionnalités requises et des autorisations différentes avant de pouvoir sélectionner différents VPC ou GKE.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage (Gestion)** > **Workloads(Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **GCP connector** (connecteur GCP).

Étape 3 Si vous avez plusieurs connecteurs GCP, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, reportez-vous à Configurer un connecteur GCP, à la page 268.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données GKE), vous devez télécharger le modèle IAM révisé et le charger dans GKE avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez rempli les conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 272. Dans la page qui répertorie les VPC, sélectionnez **Enable Segmentation** (activer la segmentation) pour les VPC sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des VPC sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this step** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser)** > **Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portée pour les VPC sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parentale au-dessus de l'arborescence des portées, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données GCP

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP

Avertissement Avant d'activer l'application de la segmentation sur un VPC, créez une sauvegarde des groupes de sécurité sur ce VPC. L'activation de la segmentation pour un VPC supprime les groupes de sécurité existants de ce VPC. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité.

Lors de la création de politiques :

- Comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.
- Parce que GCP autorise les deux règles ALLOW/DENY (AUTORISER/REFUSER) dans la politique de pare-feu. Depuis, GCP a une limitation très stricte sur le nombre de règles. Donc, il est préférable d'avoir uniquement la liste ALLOW.

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le VPC associé. Si vous activez la segmentation pour un VPC qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce VPC.

Lorsque vous êtes prêt à appliquer des politiques pour un VPC, modifiez le connecteur GCP (voir Modifier un connecteur GCP, à la page 271) et activez la segmentation pour ce VPC.

Étiquettes d'inventaire de GKE, détails et état d'application

Pour afficher des informations sommaires sur un connecteur GCP, accédez à **Connector >** et choisissez GCP Connector (Connecteur GCP) dans la page Connectors (Connecteurs).

Pour afficher des informations sur l'inventaire, cliquez sur l'adresse IP d'une charge de travail particulière dans la page Scopes and Inventory (Portée et inventaire). Vous pouvez également accéder au profil d'inventaire à partir de l'onglet d'interface du profil VPC. Pour en savoir plus sur le profil d'inventaire, consultez Profil d'inventaire.

De même, pour afficher toutes les politiques concrètes sous le profil VPC, sous l'onglet Politiques concrètes du profil d'inventaire, accédez au profil VPC parent pour voir toutes les politiques concrètes sous le VPC.

Le profil VPC est accessible à partir de la page de configuration ou d'état d'application GCP (globale ou au sein d'un espace de travail). Vous pouvez afficher l'état de l'application et les politiques concrètes au niveau du VPC sur le profil VPC. Vous pouvez également afficher les politiques de pare-feu VPC combinées de toutes les interfaces dans l'onglet VPC Firewall Rules (politiques de pare-feu VPC).

Pour en savoir plus sur les étiquettes, consultez :

- Étiquettes générées par les connecteurs infonuagiques

- Étiquettes liées aux grappes Kubernetes

Résoudre les problèmes de connecteur GCP

Problème : La page Enforcement Status (État de la mise en application) indique qu'une politique concrète a été SKIPPED (IGNORÉE).

Solution : Ce problème se produit lorsque le nombre de règles dans la politique de pare-feu dépasse les limites GCP, telles que configurées dans le connecteur GCP.

Lorsqu'une politique concrète s'affiche comme SKIPPED (IGNORÉE), les nouveaux groupes de sécurité ne sont pas mis en œuvre et les groupes de sécurité existants sur GCP restent en vigueur.

Pour résoudre ce problème, voyez si vous pouvez consolider les politiques, par exemple en utilisant un sous-réseau plus grand dans une politique plutôt que plusieurs avec des sous-réseaux plus petits.

Contexte :

Des politiques concrètes sont générées pour chaque VPC lorsque la segmentation est activée. Ces politiques concrètes sont utilisées pour créer des politiques de pare-feu dans GCP. Cependant, GCP et Cisco Secure Workload comptabilisent les politiques différemment. Lors de la conversion de politiques Cisco Secure Workload en règles de pare-feu GCP dans les politiques de pare-feu, le mécanisme de comptage GCP est complexe. Pour plus de renseignements, voir GCP.

Problème : GCP autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes s'exécutant sur GCP (GKE)

Vous pouvez utiliser un connecteur infonuagique pour recueillir des métadonnées à partir des grappes Google Kubernetes Engine (GKE) s'exécutant sur Google Cloud Platform (GCP).

Le connecteur rassemble toutes les métadonnées de nœuds, de services et d'espaces liées à toutes les grappes Kubernetes sélectionnées.

Exigences et prérequis

Exigences de Cisco Secure Workload : ce connecteur ne nécessite pas d'appliance virtuelle.

Exigences de la plateforme :

- Assurez-vous que vous disposez des autorisations dans GCP pour configurer l'accès requis pour ce connecteur.
- Chaque grappe GKE ne peut appartenir qu'à un seul connecteur GCP.
- Recueillez les informations décrites dans les tableaux de la section *Configurer un connecteur GCP*, ci-dessous.

Exigences GKE :

- Vous devez configurer les privilèges d'accès requis dans GKE.
- Pour prendre en charge les fonctionnalités des K8 gérés, les rôles requis par le compte de service sont les suivants :

- Le Compute Network Viewer (Visualiseur de réseau informatique) est un rôle IAM qui donne un accès en lecture seule à toutes les ressources réseau dans GCP.https://cloud.google.com/compute/docs/access/iam#compute.networkViewer
- Le Kubernetes Engine Viewer (Visualiseur de moteur Kubernetes) est un rôle de grappe GKE qui fournit un accès en lecture seule aux ressources des grappes GKE, telles que les nœuds, les pods et les objets d'API GKE. https://cloud.google.com/iam/docs/understanding-roles#kubernetes-engine-roles

Connecteurs d'identité

Le connecteur d'identités sert de pont entre Cisco Secure Workload et divers entrepôts d'identités, tels qu'OpenLDAP, Active Directory et Azure AD. Le connecteur vous permet de synchroniser les renseignements stockés dans les entrepôts d'identités sans intervention manuelle. Actuellement, vous pouvez configurer un connecteur d'identité pour acquérir les données des utilisateurs à partir de LDAP.

Configurer un connecteur OpenLDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole conçu pour récupérer des informations sur les utilisateurs, les groupes d'utilisateurs, les organisations et d'autres attributs. Son objectif principal est de stocker des données dans l'annuaire LDAP pour rationaliser la gestion des utilisateurs.

Note La version prise en charge pour l'acquisition de données OpenLDAP est OpenLDAP 2.6.

Configuration

Créez un connecteur d'identité pour LDAP dans Cisco Secure Workload afin d'établir la communication avec OpenLDAP.

Procédure

Étape 1 Dans le volet de navigation, choisissez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Connectors (Connecteurs)** .

Étape 2 Sélectionnez **Identity Connector** (Connecteur d'identité) et cliquez sur **Configure your new connector here** (Configurez votre nouveau connecteur ici).

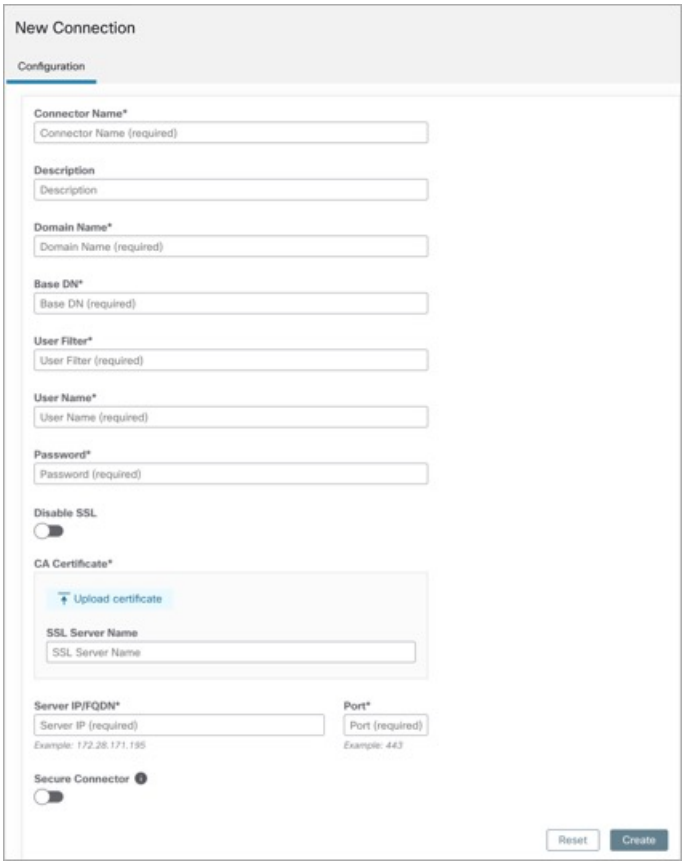
Étape 3 Sur la page **New Connection** (Nouvelle connexion), saisissez les détails comme suit :

Champs	Description
Nom du connecteur	Saisissez un nom pour le connecteur.
Description	Saisissez une description
Domain Name (Nom de domaine)	Saisissez un nom de domaine Le nom de domaine doit être unique dans la portée sélectionnée. Par exemple, csw.com.

Champs	Description
Nom unique de base	Saisissez le DN de base ou le nom distinctif qui sert de point de départ aux recherches dans l'arborescence. Par exemple, dc=csw, dc=com.
Filtre utilisateur	Saisissez un filtre pour définir des critères d'identification des entrées qui contiennent certains types de renseignements. Exemple 1 : pour identifier des utilisateurs, vous les distinguez en utilisant deux attributs objetClass, l'un défini sur « person » et l'autre sur « user ». Les critères de correspondance peuvent être `(&(objectClass=person)(objectClass=user))` Exemple 2 : pour récupérer toutes les entrées qui ont pour objet class=user et l'attribut « cn » contenant le mot « Marketing », le filtre de recherche peut être `(&(ObjectClass=user)(cn=*Marketing*))`
Nom d'utilisateur et **mot de passe**	Saisissez les renseignements d'authentification pour vous connecter au serveur OpenLDAP.
Certificat de l'autorité de certification	Chargez le certificat de l'autorité de certification et entrez le nom du serveur SSL utilisé par Cisco Secure Workload pour l'authentification. Sinon, **désactivez SSL**.
Server IP/FQDN and Port (Adresse IP du serveur/Nom de domaine complet et Port)	Saisissez l'adresse IP du serveur et le numéro de port.
Connecteur sécurisé	Activez si un connecteur sécurisé est utilisé pour canaliser les connexions de Cisco Secure Workload vers OpenLDAP. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé. Pour en savoir plus, consultez la section Connecteur sécurisé

Étape 4 Cliquez sur **Create** (créer).

Illustration 103 : Configurer un nouveau connecteur



Un nouveau connecteur d'identité est créé et la communication entre Cisco Secure Workload et OpenLDAP est configurée.

Inventaire

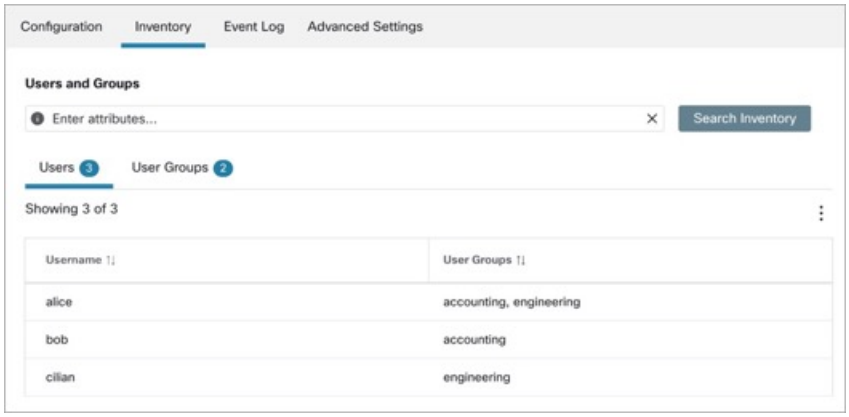
Lorsque la connexion entre Cisco Secure Workload et OpenLDAP est établie, vous pouvez afficher une liste des **utilisateurs** et **des groupes d'utilisateurs** sous l'onglet **Inventory** (inventaire). Tous les groupes d'utilisateurs auxquels un utilisateur appartient sont affichés sous l'onglet **Users** (utilisateurs). Seuls les groupes d'utilisateurs uniques sont affichés dans l'onglet User Groups (groupes d'utilisateurs).

Procédure

Étape 1 Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'information pour afficher les propriétés à filtrer.

Étape 2 Cliquez sur l'icône de menu pour télécharger les données au format JSON ou CSV.

Illustration 104 : Utilisateurs et groupes d'utilisateurs



Remarque La limite recommandée pour le nombre d'utilisateurs affichés est de 300 000, tandis que pour les groupes d'utilisateurs, elle est de 30 000.

Journal des événements

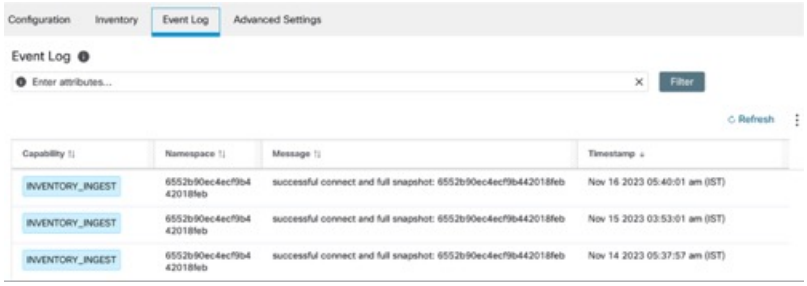
L'onglet Event Log (journal des événements) affiche des informations, des avertissements et des erreurs qui se produisent lors de l'établissement de la connexion avec OpenLDAP.

Procédure

Étape 1 Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'information pour afficher les propriétés à filtrer.

Étape 2 Cliquez sur l'icône de menu pour télécharger les données au format JSON ou CSV.

Illustration 105 : Journal des événements



Remarque Les codes de couleur des journaux sont les suivants : information (bleu), avertissement (ambre) et erreur (red).

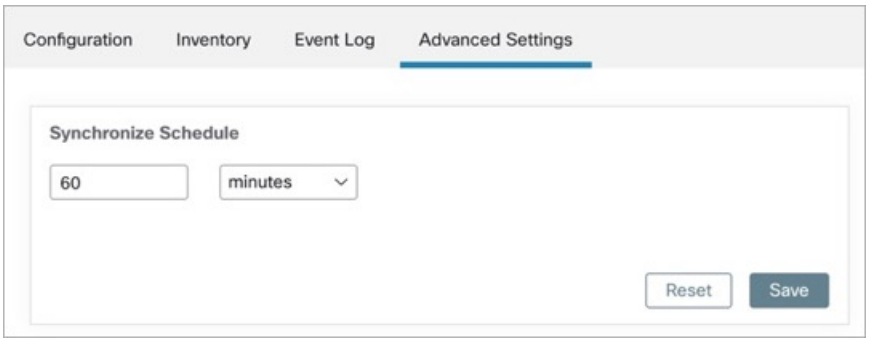
Paramètres avancés

Procédure

Étape 1 Sous **Synchronize Schedule** (Synchroniser la planification), vous pouvez choisir une fréquence à laquelle Cisco Secure Workload synchronise les données d'utilisateur à partir du serveur LDAP.

Étape 2 Dans le champ **User Attributes** (attributs de l'utilisateur), saisissez jusqu'à six attributs utilisateur à afficher.

Illustration 106 : Paramètres avancés



Alertes du connecteur

Un appareil ou un service crée une alerte de connecteur lorsqu'il présente un comportement anormal.

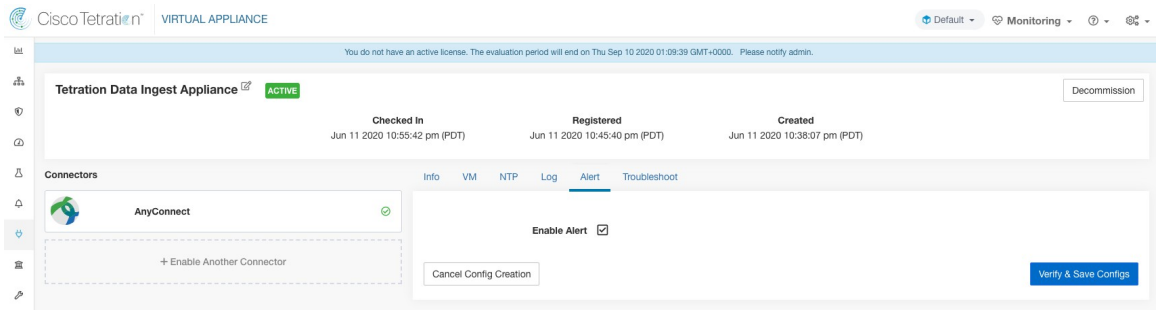
Configuration des alertes

La configuration des alertes pour les appareils et les connecteurs vous permet de générer des alertes pour divers événements. Dans la version 3.4, cette configuration active tous les types d'alertes potentiellement possibles pour l'appareil/connecteur configuré.

Nom du paramètre	Type	Description
Enable Alert	case	L'alerte doit-elle être activée?

Note La valeur par défaut pour *Enable Alert* est *vrai*.

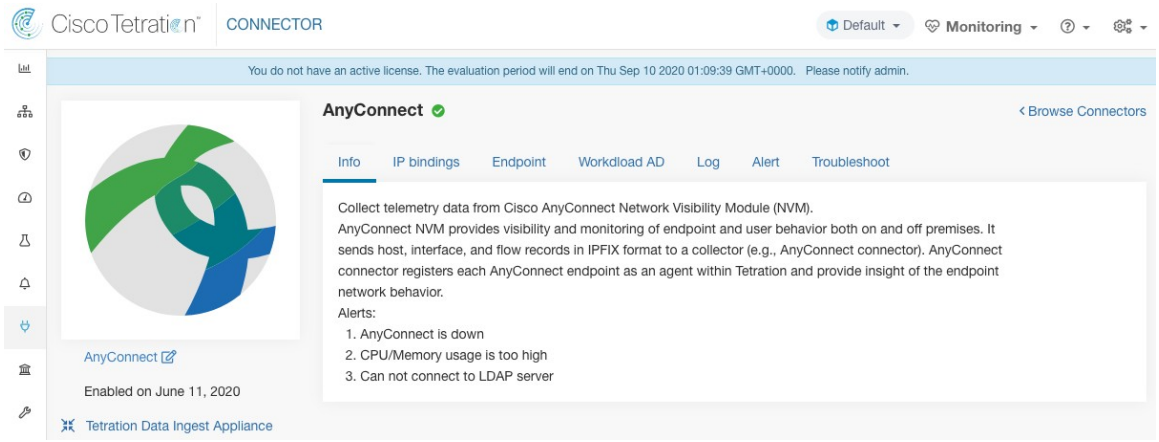
Figure 107: Afficher la configuration des alertes sur un appareil d'acquisition de données Cisco Secure Workload



Type d'alerte

L'onglet Info des pages de l'appareil et du connecteur contient différents types d'alertes spécifiques à chaque appareil et connecteur.

Figure 108: Informations sur la liste d'alertes



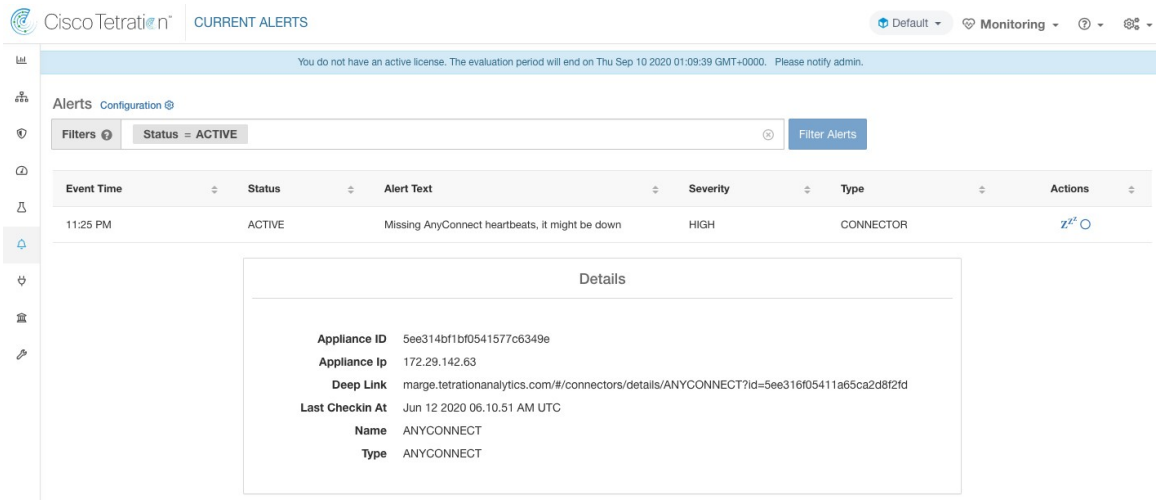
Appareil/connecteur en panne

Une alerte est générée lorsqu'un appareil (ou un connecteur) est potentiellement en panne en raison de pulsations manquantes de l'appareil ou du connecteur.

Texte d'alerte : Missing <Appliance/Connector> heartbeats, it might be down (signaux d'activité manquants <Appliance/Connector>, il est peut-être en panne).

Gravité : élevée

Figure 109: Alerte de connecteur en panne



appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : tous

Utilisation du système des appareils et des connecteurs

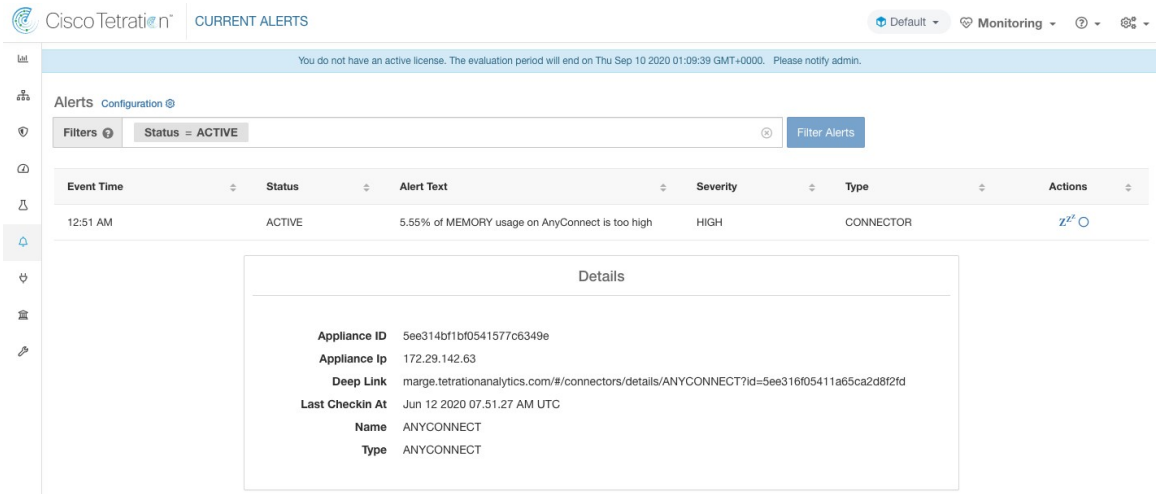
Lorsque l'utilisation du système (CPU, mémoire et disque) est supérieure à 90 % sur un appareil (et un connecteur). L'appareil (et/ou le connecteur) génère une alerte informationnelle pour indiquer qu'il gère actuellement une charge système accrue.

Il est normal que les appareils et les connecteurs consomment plus de 90 % des ressources système lors d'une activité de traitement intensive.

Texte de l'alerte :<Number> d'utilisation du processeur, de la mémoire/du disque sur <Appliance/Connector> est trop élevé.

Gravité : élevée

Figure 110: Alerte d'utilisation du système du connecteur trop élevée



appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : tous

Erreur de configuration du connecteur

Lorsque vous essayez de connecter un connecteur configuré à un serveur configuré et que la configuration échoue, le système génère une alerte pour indiquer un problème potentiel de configuration après son acceptation et son déploiement.

Par exemple, le connecteur AnyConnect peut accepter une configuration LDAP, valider et accepter la configuration. Cependant, pendant le fonctionnement normal, il est possible que la configuration ne soit plus valide.

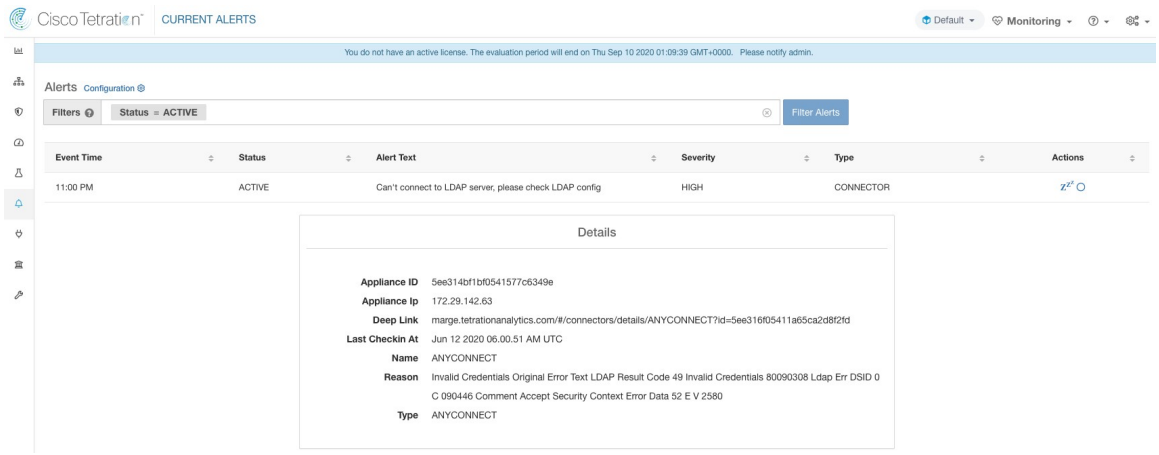
Une alerte capture le scénario et indique que vous devez prendre des mesures correctives pour mettre à jour la configuration.

Texte d'alerte : Impossible de se connecter au serveur <Appareil/Connecteur>, vérifier la configuration de <Appareil/Connecteur>.

Gravité : élevée, faible

Serveur	Connecteur
Serveur LDAP	AnyConnect, F5, ISE, WDC
Serveur ISE	ISE
Serveur ServiceNow	ServiceNow

Figure 111: Alerte pour erreur d'état de configuration

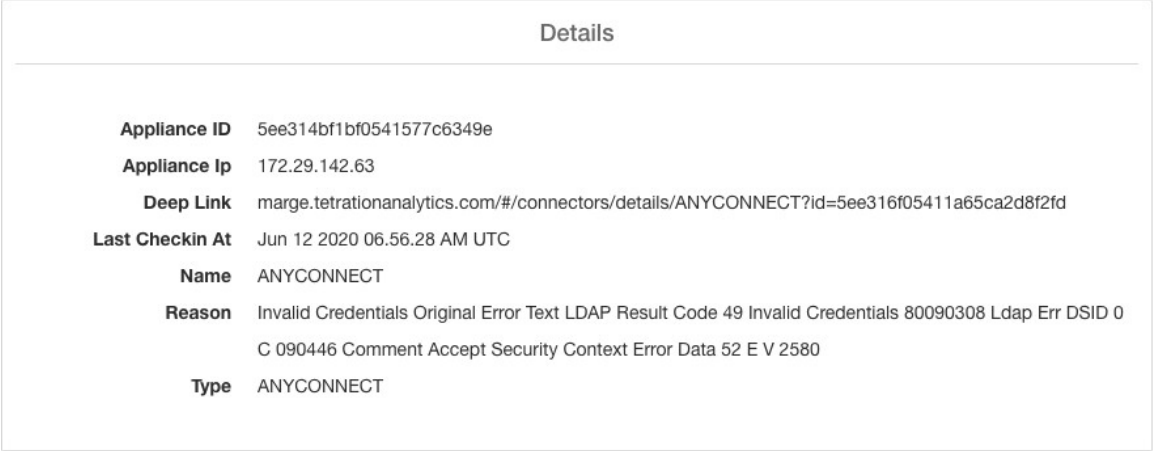


appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : AnyConnect, F5, ISE, WDC et ServiceNow.

Détails de l'alerte de l'interface utilisateur du connecteur

Figure 112: Détails de l'alerte de l'interface utilisateur du connecteur



Détails de l'alerte

Consultez Structure commune des alertes pour obtenir la structure générale des alertes et des informations sur les champs. La structure des champs *alert_details* contient les sous-champs suivants pour les alertes de connecteur.

Champ	Type	Description
ID de dispositif	Chaîne	ID de dispositif
IP d'appareil	Chaîne	IP d'appareil
ID du connecteur	Chaîne	ID du connecteur
Adresse IP du connecteur	Chaîne	Adresse IP du connecteur
Lien profond	Lien hypertexte	Redirection vers la page de l'appareil/du connecteur
Last CheckIn At	Chaîne	Heure de la dernière connexion
Nom	Chaîne	Nom de l'appareil/du connecteur
Motif	Chaîne	Raison pour laquelle l'appareil ou le connecteur ne peut pas se connecter à Cisco Secure Workload
Type	Chaîne	Type d'appareil/de connecteur

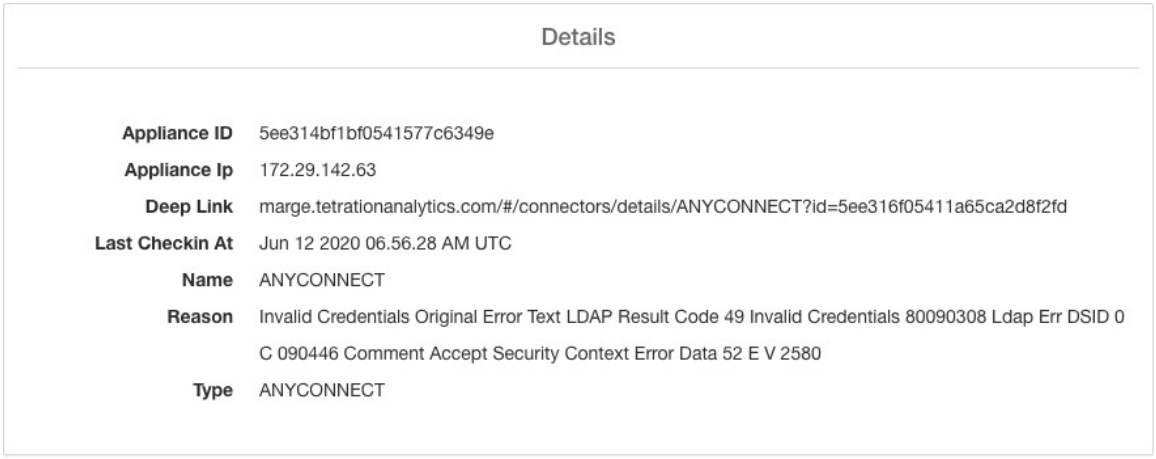
Exemple de détails d'alerte

Après avoir analysé alert_details comme JSON (n'est pas une chaîne), il s'affichera comme suit.

```
    {
      "Appliance ID": "5f1f3d26d674b01832c6792a",
      "Connector ID": "5f1f3e47baba512a70abee43",
      "Connector IP": "172.29.142.22",
      "Deep Link":
"bingo.tetrationanalytics.com/#/connectors/details/F5?id=5f1f3e47baba512a70abee43",
      "Last checkin at": "Aug 04 2020 20.37.33 PM UTC",
      "Name": "F5",
      "Reason": "Invalid Credentials (Original error text: LDAP Result Code 49 \"Invalid
Credentials\": )",
      "Type": "F5"
    }
```


Détails de l'alerte de l'interface utilisateur du connecteur

Figure 113: Détails de l'alerte de l'interface utilisateur du connecteur



Gestion du cycle de vie des connecteurs

Les connecteurs peuvent être activés, déployés, configurés, dépannés et supprimés directement à partir de Cisco Secure Workload.

Activation d'un connecteur

Sur la page Connecteurs (**Manage (Gestion)** > **Connectors (Connecteurs)**), vous pouvez sélectionner et activer un connecteur. Le connecteur peut être déployé sur une nouvelle appliance virtuelle (qui doit d'abord être mise en service et devenir *active* avant qu'un connecteur ne puisse être activé sur celle-ci) ou sur une appliance virtuelle existante. Une fois l'appliance virtuelle choisie, Cisco Secure Workload envoie le paquet RPM du connecteur à l'appliance.

Lorsque le contrôleur d'appareil sur l'appliance choisie reçoit le RPM, il effectue ce qui suit :

1. Créer une image Docker à l'aide du paquet RPM reçu de Cisco Secure Workload. Cette image Docker inclut la configuration nécessaire pour communiquer avec le sujet Kafka sur lequel les messages de gestion de l'appliance sont envoyés. Cela permet au service instancié à partir de cette image de pouvoir envoyer et recevoir des messages pour la gestion du connecteur correspondant.

2. Créer un conteneur Docker à partir de l'image Docker.
3. Sur l'appareil d'acquisition Cisco Secure Workload, les tâches supplémentaires suivantes sont effectuées.
   - Un logement (slot) libre est identifié et l'adresse IP correspondante est déterminée.
   - Les ports d'écoute des connecteurs (par exemple, les ports 4729 et 4739 sur le connecteur NetFlow pour recevoir les enregistrements de flux de commutateurs et de routeurs compatibles avec NetFlow V9 ou IPFIX) sont accessibles à l'hôte à l'adresse IP correspondant au logement choisi.
   - Un volume Docker est créé et ajouté au conteneur.
4. Le conteneur Docker est démarré et il exécute le connecteur en tant que service géré *surveillé*. Le service démarre *le contrôleur de services* en tant que *tet-controller,* qui s'enregistre auprès de Cisco Secure Workload et génère le service de connecteur proprement dit.

Figure 114: Images de Docker

```
[root@beretta-ingest-1 tetter]# docker images
REPOSITORY                                                TAG                 IMAGE ID            CREATED             SIZE
netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow    5d379fac6e37d85f2bdeff45   2635145b44c8        About a minute ago   650MB
tet-service-base                                          latest              6be171bbe648        4 days ago          519MB
artifacts.tet.wtf:6555/centos                             7.3.1611            c5d48e81b986        4 months ago        192MB
[root@beretta-ingest-1 tetter]#
```

Figure 115: Volumes de Docker

```
[root@beretta-ingest-1 tetter]# docker volume ls
DRIVER              VOLUME NAME
local               373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439
[root@beretta-ingest-1 tetter]#
```

Figure 116: Conteneurs Docker

```
[root@beretta-ingest-1 tetter]# docker ps
CONTAINER ID        IMAGE                                                                                                COMMAND                  CREATE
D              STATUS              PORTS                                                                  NAMES
2c7a7ed4f853        netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45   "/usr/bin/supervisor…"   About
a minute ago   Up About a minute   172.29.142.26:4729->4729/udp, 172.29.142.26:4739->4739/udp   nf-5d379fac6e37d85f2bdeff45
[root@beretta-ingest-1 tetter]#
```

Figure 117: Logement utilisé par le conteneur Docker et liste des ports accessibles


```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


Figure 118: Liste des ports rendus accessibles par le conteneur Docker


```
[root@beretta-ingest-1 tetter]# docker port 2c7a7ed4f853
4729/udp -> 172.29.142.26:4729
4739/udp -> 172.29.142.26:4739
[root@beretta-ingest-1 tetter]#
```


Figure 119: Volume Docker monté sur un conteneur


```
[root@beretta-ingest-1 tetter]# docker inspect --format='{{json .Mounts}}' 2c7a7ed4f853
[{"Type":"volume","Name":"373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439","Source":"/var/lib/docker/volumes/373b5b6
82a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439/_data","Destination":"/local/tetration","Driver":"local","Mode":"z","RW":tr
ue,"Propagation":""}]
[root@beretta-ingest-1 tetter]#
```


Le contrôleur de services est responsable des fonctions suivantes :

1. **Registration**(enregistrement) : enregistre le connecteur auprès de Cisco Secure Workload. Tant que le connecteur n'est pas enregistré et marqué *Enabled* (activé), aucune mise à jour de configuration ne peut

être envoyée au connecteur. Lorsque Cisco Secure Workload reçoit une demande d'enregistrement pour un connecteur, il met à jour l'état du connecteur à *Enabled* (activé).

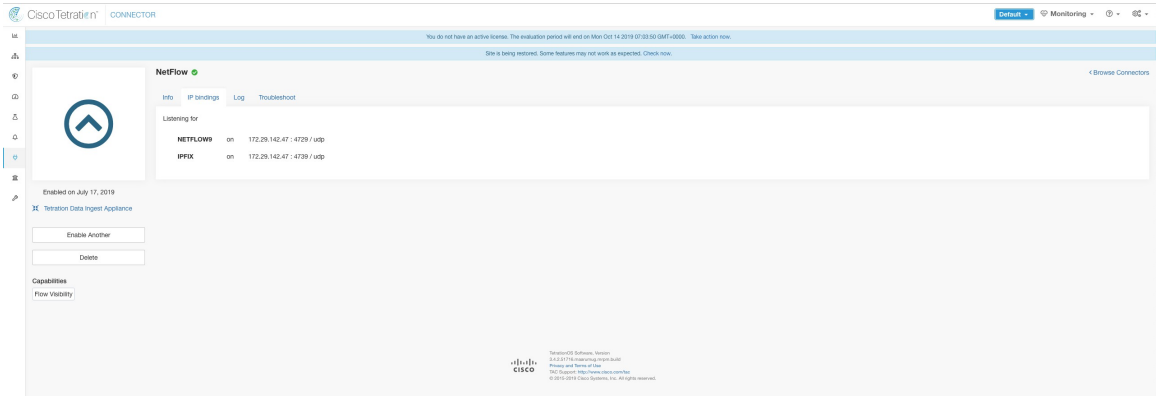
2. **Mises à jour de la configuration sur le connecteur** : teste et applique les mises à jour de configuration sur le connecteur. Pour en savoir plus, consultez Gestion de la configuration sur les connecteurs et les appliances virtuelles.
3. **Commandes de dépannage sur le connecteur** : exécute les commandes autorisées sur le service de connecteur pour le dépannage et le débogage des problèmes sur le service de connecteur. Consultez la section Dépannage (Dépannage) pour en savoir plus.
4. **Heartbeats** (pulsations) : envoie régulièrement des pulsations et des statistiques à Cisco Secure Workload pour signaler l'intégrité du connecteur. Pour en savoir plus, consultez Surveillance d'une appliance virtuelle.

Affichage des informations relatives au connecteur

Connecteurs activés : Vous pouvez obtenir une liste de tous les connecteurs activés en cliquant sur **Manage (Gestion)** > **Connectors (Connecteurs)** dans la barre de navigation à gauche de la fenêtre.

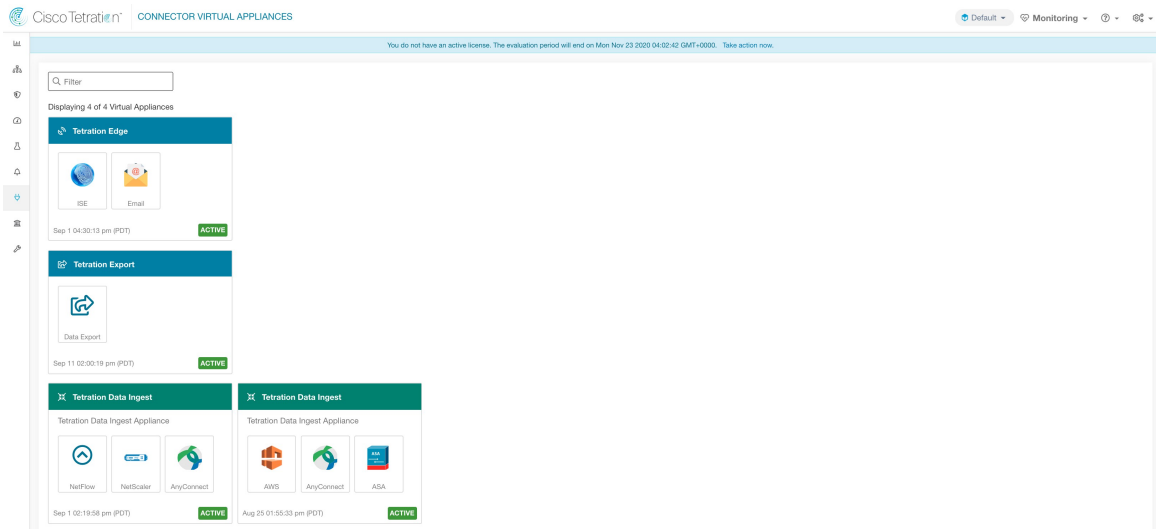
Détails du connecteur : Vous pouvez obtenir des détails sur le connecteur en cliquant sur le connecteur. Cette page affiche les liaisons de port (le cas échéant) qui peuvent être utilisées pour configurer les éléments de réseau en amont afin d'envoyer des données de télémétrie à l'adresse IP et au port appropriés.

Figure 120: Détails du connecteur



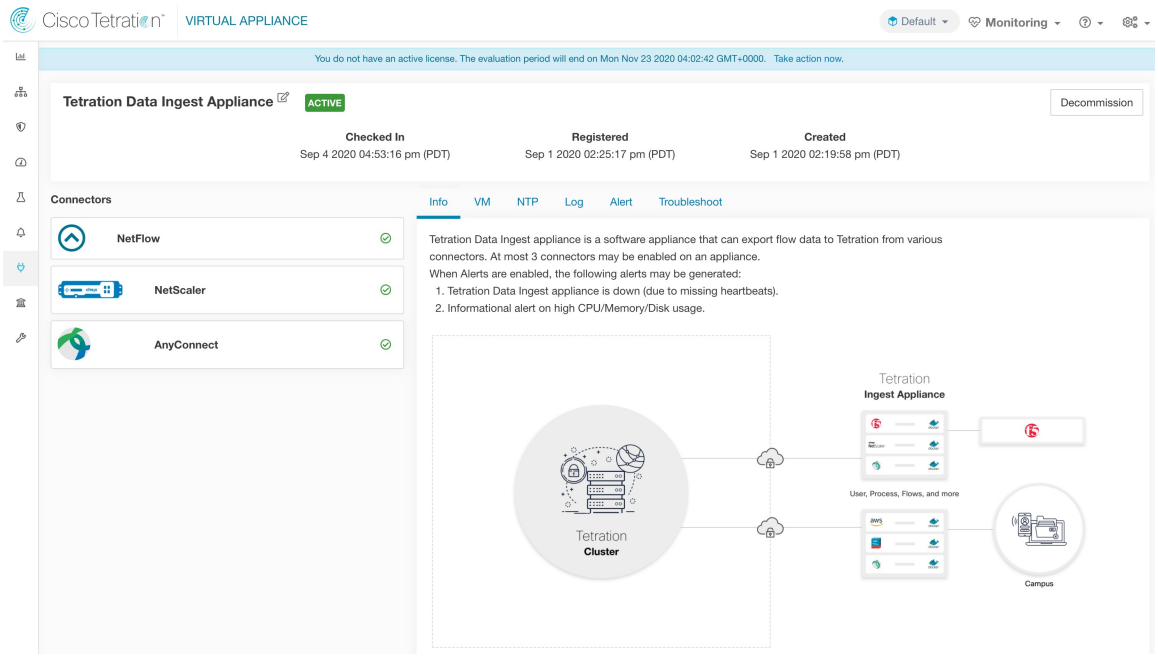
Appliances virtuelles déployées : Vous trouverez une liste des appliances virtuelles déployées à l'adresse suivante : **Manage (Gestion)** > **Virtual Appliances (Appliances virtuelles)** .

Figure 121: Liste des appliances virtuelles déployées



Détails de l'appliance virtuelle Pour obtenir une vue détaillée d'une appliance, cliquez sur celle-ci directement dans la *Liste des appliances virtuelles déployées*.

Figure 122: Détails sur l'appliance et les connecteurs



Suppression d'un connecteur

Lorsqu'un connecteur est supprimé, le contrôleur d'appareil sur l'appareil où le connecteur est activé reçoit un message lui demandant de supprimer les services créés pour le connecteur. Le contrôleur de l'appareil effectue les tâches suivantes :

1. Arrêter le conteneur Docker correspondant au connecteur.
2. Supprimer le conteneur Docker.
3. Si le connecteur est déployé sur un appareil d'acquisition Cisco Secure Workload et qu'il expose des ports, retirer le volume Docker qui a été monté sur le conteneur.
4. Supprimer l'image Docker qui a été créée pour le connecteur.
5. Enfin, renvoyer un message à Cisco Secure Workload pour indiquer l'état de la demande de suppression.

Surveillance d'un connecteur

Les services du connecteur envoient régulièrement des signaux de présence et des statistiques à Cisco Secure Workload. L'intervalle du signal de présence (heartbeat) est de 5 minutes. Les messages heartbeat comprennent des statistiques sur l'intégrité du service, notamment des statistiques du système, des statistiques de processus et des statistiques sur le nombre de messages envoyés, reçus ou erronés sur le sujet Kafka utilisé pour la gestion de l'appareil. En outre, ils comprennent les statistiques exportées par le service de connecteur lui-même.

Toutes les métriques sont disponibles dans *Digger* (OpenTSDB) et sont annotées avec l'ID de l'appareil, l'ID du connecteur et le nom de la portée racine. En outre, les tableaux de bord Grafana pour les services du connecteur sont également disponibles pour les mesures importantes du service.

Appliances virtuelles pour les connecteurs

La plupart des connecteurs sont déployés sur des appliances virtuelles Cisco Secure Workload. Vous déploierez les appareils virtuels requis sur un hôte ESXi dans VMware vCenter en utilisant les modèles OVA ou sur d'autres hyperviseurs basés sur KVM à l'aide de l'image QROW2. La procédure de déploiement d'appliances virtuelles est décrite dans la section Deploying a Virtual Appliance.

Types d'appliances virtuelles

Chaque connecteur nécessitant une appliance virtuelle peut être déployé sur l'un des deux types d'appliances virtuelles.

Acquisition de Cisco Secure Workload

L'appareil d'acquisition Cisco Secure Workload est une appliance logicielle qui peut exporter des observations de flux vers Cisco Secure Workload à partir de divers connecteurs.

Fiche technique

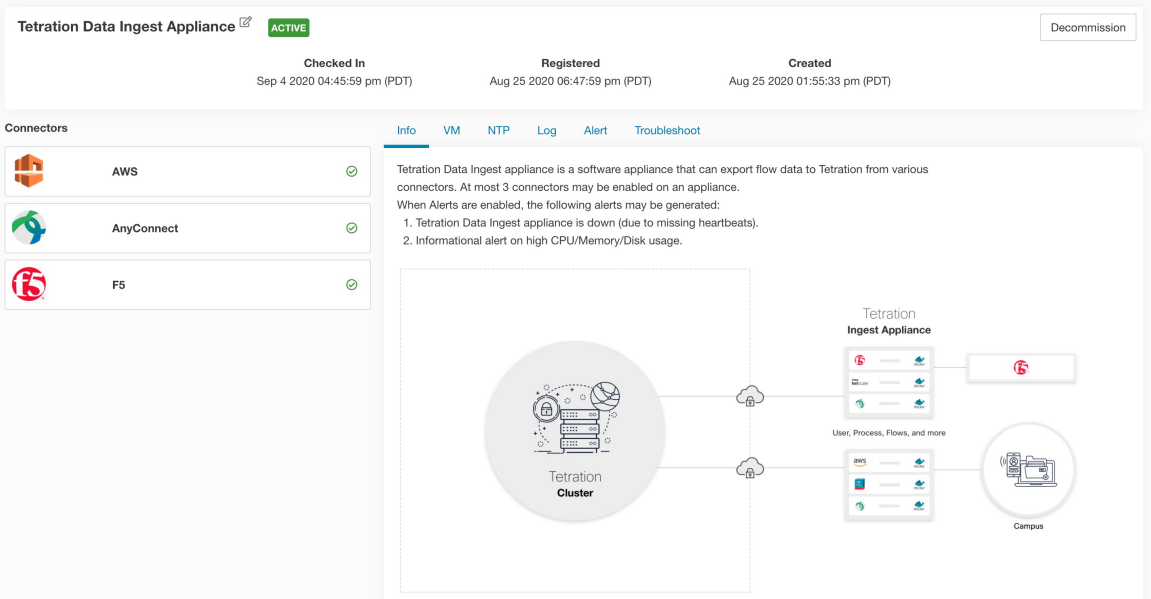
- Nombre de cœurs de processeur : 8
- Mémoire : 8 Go
- Stockage : 250 Go
- Nombre d'interfaces réseau : 3
- Nombre de connecteurs sur un appareil : 3

- Système d'exploitation : CentOS 7.9 (Cisco Secure Workload 3.8.1.19 et versions ultérieures), AlmaLinux 9.2 (Cisco Secure Workload 3.8.1.36 ou versions ultérieures)

Consultez les limites importantes à l'adresse Connecteurs.

Note Chaque portée racine sur Cisco Secure Workload ne peut avoir qu'un maximum de 100 dispositifs d'acquisition Cisco Secure Workload déployés.

Figure 123: Dispositif d'acquisition Cisco Secure Workload



L'appareil d'acquisition Cisco Secure Workload permet à un maximum de trois connecteurs d'être activés sur un dispositif. Plusieurs instances d'un même connecteur peuvent être activées sur le même appareil. Pour l'appareil d'acquisition ERSPAN, trois connecteurs ERSPAN sont toujours mis en service automatiquement. Un grand nombre des connecteurs déployés sur l'appareil d'acquisition collecte la télémétrie de divers points du réseau. Ces connecteurs doivent être à l'écoute sur des ports spécifiques de l'appareil. Chaque connecteur est par conséquent lié à l'adresse IP et au port par défaut sur lequel le connecteur doit être à l'écoute pour collecter des données de télémétrie. Par conséquent, chaque adresse IP est essentiellement un emplacement qu'un connecteur occupe sur l'appareil. Lorsqu'un connecteur est activé, un emplacement est occupé (et donc l'adresse IP correspondant à l'emplacement). De plus, lorsqu'un connecteur est désactivé, l'emplacement occupé par le connecteur est libéré (et donc l'adresse IP correspondant à l'emplacement). Reportez-vous à la section relatives à *l'acquisition de Cisco Secure Workload* pour savoir comment l'appareil d'acquisition assure la maintenance de l'état des emplacements.

Figure 124: Emplacements de l'appareil d'acquisition Cisco Secure Workload


```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


Configurations autorisées

- *NTP* : configurez le NTP sur l'appareil. Pour en savoir plus, consultez Configuration du protocole NTP.
- *Log (Journal)* : Configurez la journalisation sur l'appareil. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Cisco Secure Workload Edge

Cisco Secure Workload Edge est un appareil de contrôle qui transmet des alertes à divers notifications et recueille les métadonnées d'inventaire provenant de contrôleurs d'accès réseau comme Cisco ISE. Dans un appareil de périphérie Cisco Secure Workload, tous les connecteurs de notification d'alerte (comme Syslog, Courriel, Slack, PagerDuty et Kinesis), le connecteur ServiceNow, le connecteur de charge de travail AD et le connecteur ISE, peuvent être déployés.

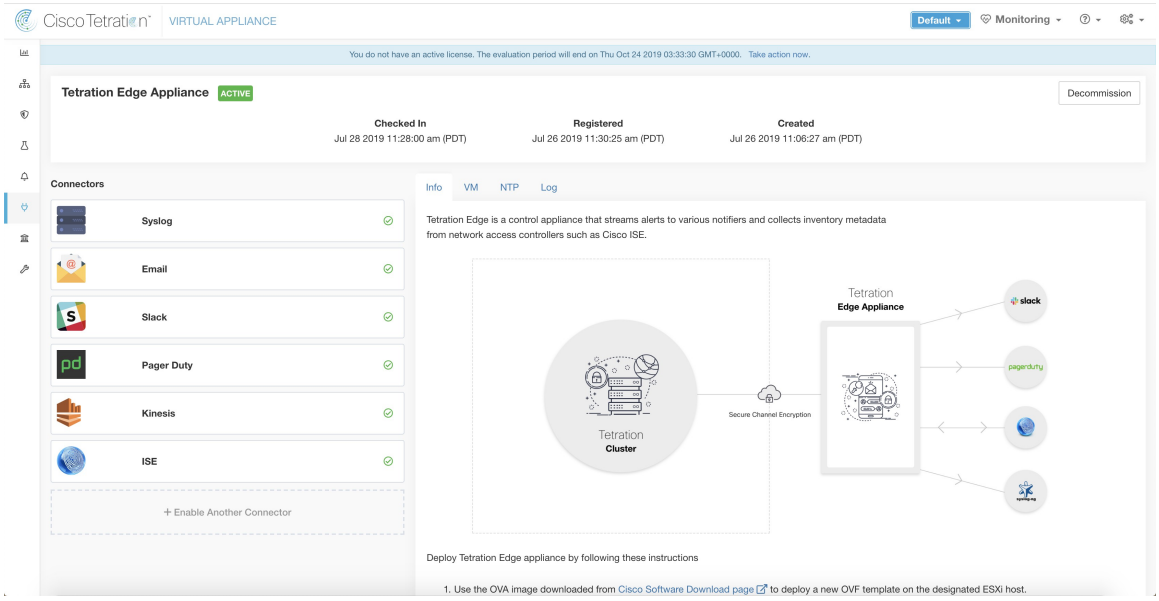
Fiche technique

- Nombre de cœurs de processeur : 8
- Mémoire : 8 Go
- Stockage : 250 Go
- Nombre d'interfaces réseau : 1
- Nombre de connecteurs sur un appareil : 8
- Système d'exploitation : CentOS 7.9 (Cisco Secure Workload 3.8.1.19 et versions ultérieures), AlmaLinux 9.2 (Cisco Secure Workload 3.8.1.36 ou versions ultérieures)

Consultez les limites importantes à l'adresse Connecteurs.

Note Chaque portée racine sur Cisco Secure Workload ne peut avoir qu'un seul appareil de périphérie Cisco Secure Workload déployé.

Figure 125: Appareil de périphérie Cisco Secure Workload



Les connecteurs déployés sur l'appareil de périphérie Cisco Secure Workload n'écoutent pas sur les ports. Par conséquent, les conteneurs Docker instanciés pour les connecteurs sur l'appareil de périphérie Cisco Secure Workload n'exposent aucun port à l'hôte.

Configurations autorisées

- *NTP* : configurez le NTP sur l'appareil. Pour en savoir plus, consultez Configuration du protocole NTP.
- *Log (Journal)* : Configurez la journalisation sur l'appareil. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Deploying a Virtual Appliance

You will deploy virtual appliances on an ESXi host in VMware vCenter or other KVM-based hypervisors such as Red Hat Virtualization. This procedure will prompt you to download virtual appliance OVA template or QCOW2 image from the Cisco Software Download page.

Attention To deploy a Cisco Secure Workload external appliance, the ESXi host where the appliance is created should have the following specifications:

- **vSphere**: version 5.5 or better.
- **CPU**: at least 2.2 GHz per core, and has enough reservable capacity for the appliance.
- **Memory**: at least enough space to fit the appliance.

To deploy a virtual appliance to collect data from connectors:

Procedure

Étape 1 In the Cisco Secure Workload web portal, choose **Manage** > **Virtual Appliances** from the navigation bar on the left.

Étape 2 Click **Enable a Connector**. The type of virtual appliance you need to deploy depends on the type of connector you are enabling.

Étape 3 Click the type of connector for which you need to create the virtual appliance. For example, click the NetFlow connector.

Étape 4 On the connector page, click **Enable**.

Étape 5 If you see a notice telling you that you need to deploy a virtual appliance, click **Yes**. If you do not see this notice, you may already have a virtual appliance that this connector can use, in which case you do not need to perform this procedure.

Étape 6 Click the link to download the OVA template or QCOW2 image for the virtual appliance. Leave the wizard open on your screen without clicking anything else.

Étape 7 Use the downloaded:

- OVA to deploy a new OVF template on a designated ESXi host.
  - Please follow Deploy an OVF Template for instructions on how to deploy an OVA on a vSphere Web Client.
  - Ensure that the deployed VM settings match the recommended configuration for the virtual appliance type.
  - **Do not power on the deployed VM**
- QCOW2 image to create a new VM on KVM hypervisors such as Red Hat Virtualization.

Étape 8 After the VM is deployed, but before you power it on, return to the virtual appliance deployment wizard in the Cisco Secure Workload web portal.

Étape 9 Click **Next** in the virtual appliance deployment wizard.

Étape 10 Configure the virtual appliance by providing IP address(es), gateway(s), hostname, DNS, proxy server settings and docker bridge subnet configuration. Please refer to the screenshot for *Configuring the VM with network parameters*.

Note For NetFlow, ERSPAN, and ISE connectors, IPv6 addresses (dual stack mode) can be provided. However, do note that dual stack support is a BETA feature. For more information on the requirements and limitations for dual-stack mode, see the Cisco Cisco Secure Workload Upgrade Guide

- If the appliance needs to use proxy server to reach Secure Workload, please check the box *Use proxy server to connect to Secure Workload*. If this is not set correctly, connectors may not be able to communicate with Cisco Secure Workload for control messages, register connectors, and send flow data to Cisco Secure Workload collector.
- If the IP address(es) and gateways(s) of the appliance conflict with the default docker bridge subnet (*172.17.0.1/16*), the appliance can be configured with a customized docker bridge subnet specified in *Docker Bridge (CIDR format)* field. This requires appliance OVA 3.3.2.16 or later.

Étape 11 Click **Next**.

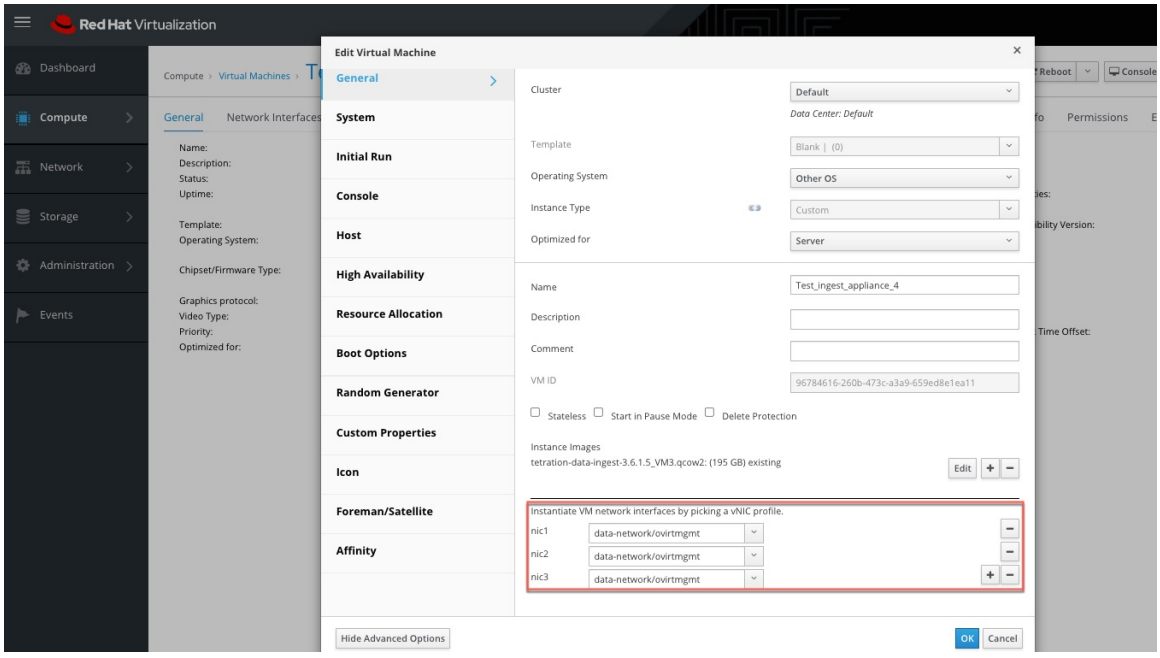
Étape 12 In the next step, a VM configuration bundle will be generated and available for download. Download the VM configuration bundle. Please refer to the screenshot for *Download the VM configuration bundle*.

Étape 13 Upload the VM configuration bundle to the datastore corresponding to the target ESXi host or other virtualization host.

Étape 14 [**Applicable only when using QCOW2 image**] Complete the following configurations on the other virutalization host where you have uploaded the VM configuration bundle:

- For ingest appliances, configure three network interfaces.

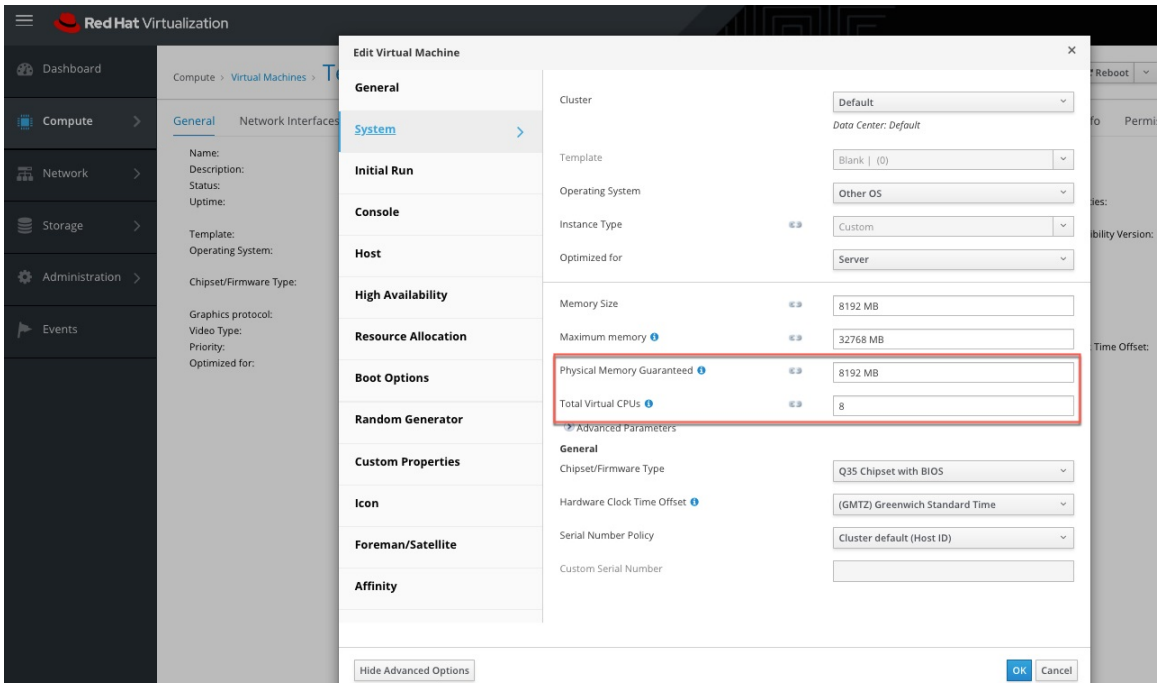
Figure 126: Example of configuring network interfaces in KVM-based environments



- In the memory allocation, specify the minimum requirement of 8192 MB of RAM.

- Specify the total number of virtual CPUs to be 8.

Figure 127: Example of configuring system resources in KVM-based environments



Étape 15 Edit the VM settings and mount the VM configuration bundle from the datastore to the CD/DVD drive. Please make sure to select **Connect at Power On** checkbox.

Étape 16 Power on the deployed VM.

Étape 17 Once the VM boots up and configures itself, it will connect back to Secure Workload. This may take a few minutes. The appliance status on Cisco Secure Workload should transition from *Pending Registration* to *Active*. Please refer to the screenshot for *Secure Workload Ingest appliance in Pending Registration state*.

Note We do not recommend vMotion to be enabled for Cisco Secure Workload external appliances.

Note We recommend to use Cisco Secure Workload external appliance OVAs as-is and to reserve 8 vCPU cores and 8192 MB of memory for QCOW2 images to deploy VMs. If sufficient resources are not available, the VM setup script would fail after the boot.

Once the appliance is *Active*, connectors can be enabled and deployed on it.

Figure 128: ploying a Cisco Secure Workload Ingest appliance

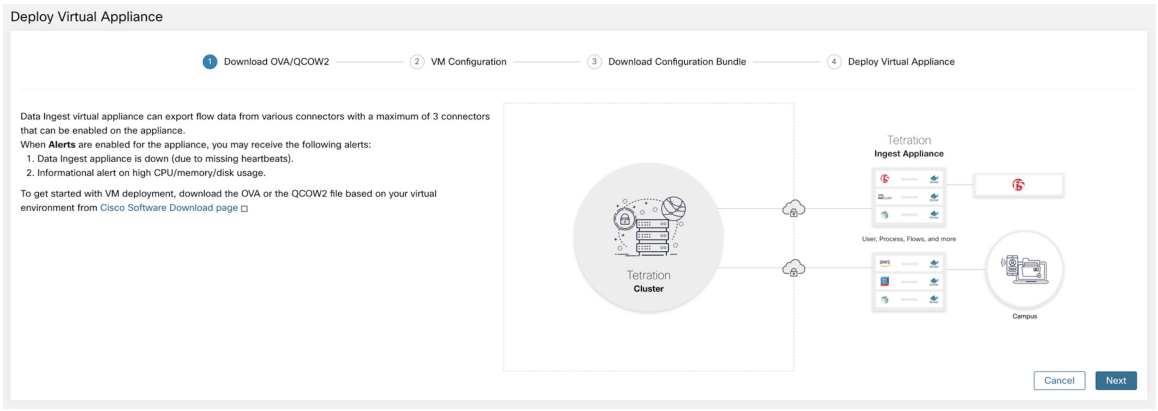


Figure 129: Configuring the VM with network parameters

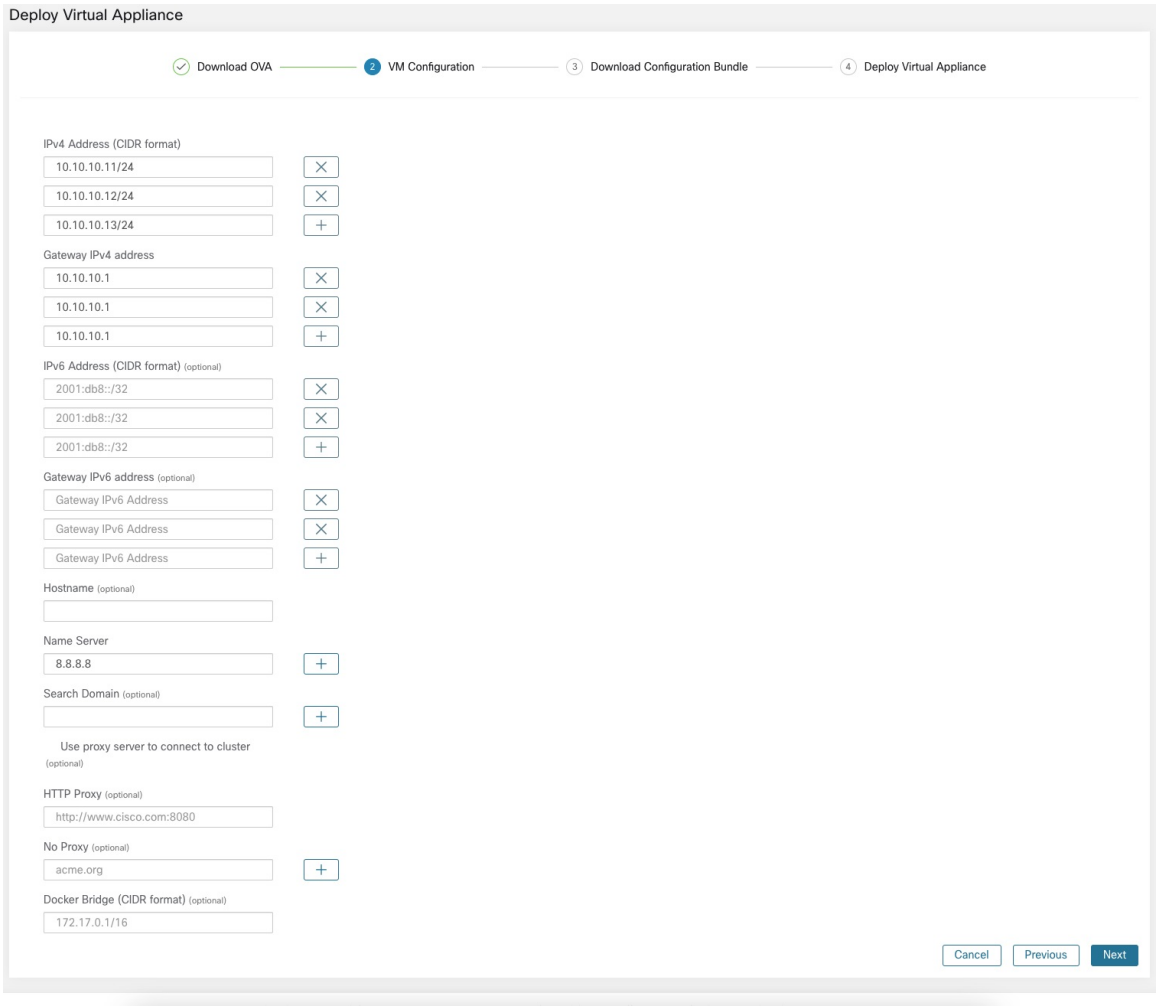


Figure 130: Download the VM configuration bundle

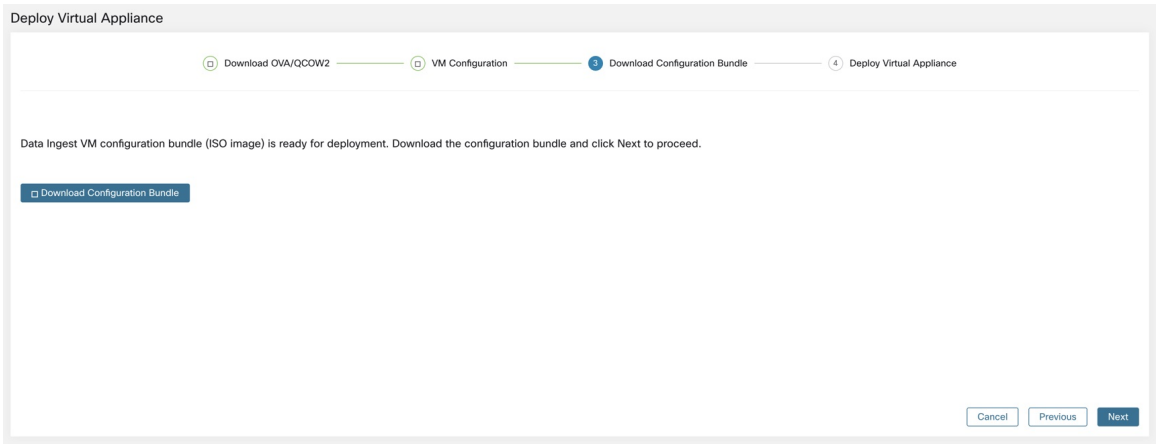


Figure 131: Deploy the VM

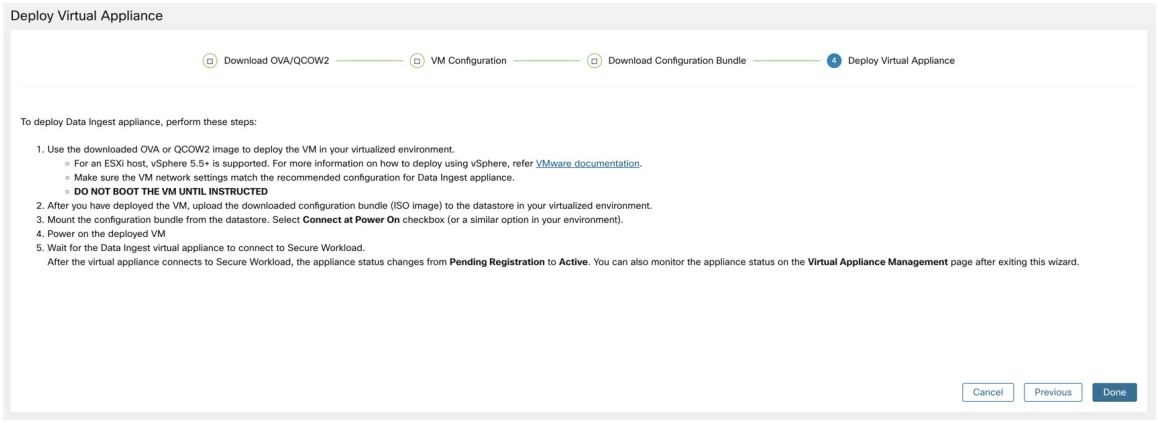
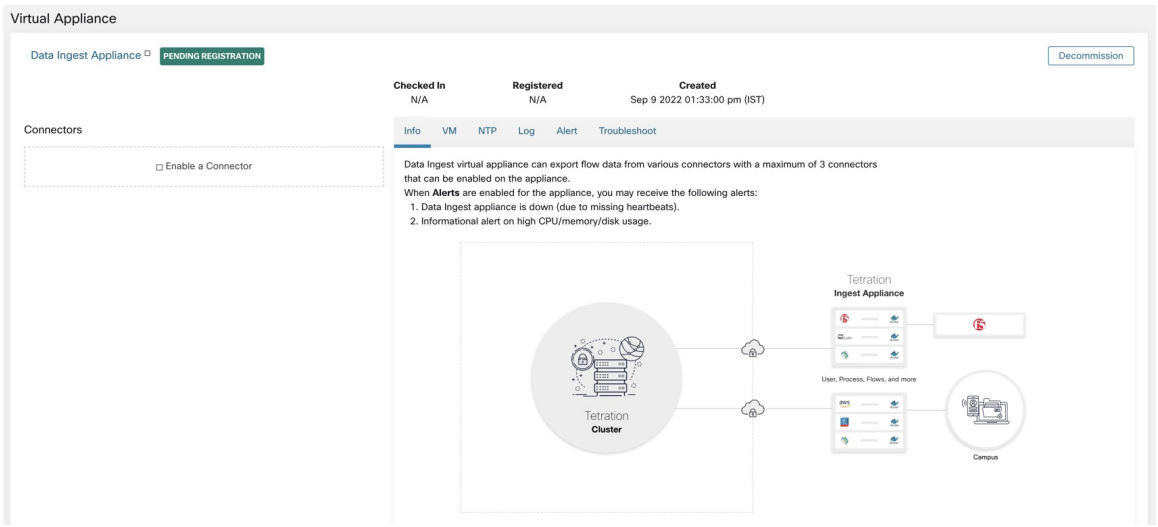


Figure 132: Cisco Secure Workload Ingest appliance in Pending Registration state



When a virtual appliance is deployed and booted up for the first time, *tet-vm-setup* service executes and sets up the appliance. This service is responsible for the following tasks

a. **Validate the appliance:** validate the appliance for mandatory resource requirements for the type of the virtual appliance deployed.

b. **IP address assignment:** assign IP addresses to all the network interfaces provisioned on the appliance.

c. **Hostname assignment:** assign hostname for the appliance (if hostname is configured).

d. **DNS configuration:** update the DNS resolv.conf file (if nameserver and/or search-domain parameters are configured).

e. **Proxy server configuration:** update HTTPS_PROXY and NO_PROXY settings on the appliance (if provided).

f. **Prepare appliance:** copies cert bundle for the Kafka topic over which appliance management messages are sent and received.

g. **Install appliance controller:** install and bring up *Appliance Controller* which is managed by *supervisord* as *tet-controller* service.

Once *tet-controller* is instantiated, it takes over the management of the appliance. This service is responsible for the following functions:

a. **Registration:** registers the appliance with Secure Workload. Until the appliance is registered, no connectors can be enabled on the appliance. When Cisco Secure Workload receives a registration request for an appliance, it updates the state of the appliance to *Active*.

b. **Deploying a connector:** deploys a connector as a Docker service on the appliance. Please refer toActivation d’un connecteur for more information.

c. **Deleting a connector:** stops and removes the Docker service and the corresponding Docker image from the appliance. Please refer to Suppression d'un connecteur for more information.

d. **Configuration updates on appliances:** tests and applies configuration updates on the appliance. Please refer to Gestion de la configuration sur les connecteurs et les appliances virtuelles for more information.

e. **Troubleshooting commands on appliances:** executes allowed set of commands on the appliances for troubleshooting and debugging issues on the appliance. Please refer to the Dépannage for more information.

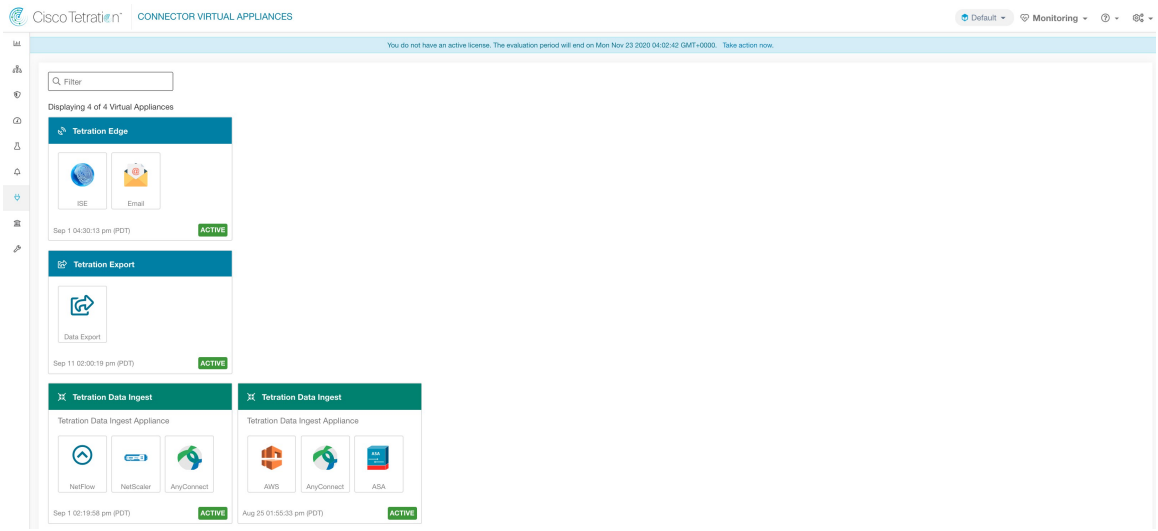
f. **Heartbeats:** periodically sends heartbeats and statistics to Cisco Secure Workload to report the health of the appliance. Please refer to Surveillance d'une appliance virtuelle for more information.

g. **Pruning:** periodically prune all Docker resources that are unused or dangling in order to recover storage space. This task is executed once every 24 hours.

h. **Decommissioning the appliance:** decommissions and deletes all Docker instances from the appliance. Please refer to Désactivation d'une appliance virtuelle for more information.

The list of deployed virtual appliances can be found at: **Manage** > **Virtual Appliances**

Figure 133: List of deployed virtual appliances



Désactivation d'une appliance virtuelle

Une appliance virtuelle peut être mise hors service dans Cisco Secure Workload. Lorsqu'une appliance est mise hors service, les actions suivantes sont déclenchées.

1. Toutes les configurations de l'appliance et les connecteurs activés sur cette dernière sont supprimés.
2. Tous les connecteurs activés sur l'appliance sont supprimés.
3. L'appliance est marquée *En attente de suppression*.
4. Lorsque l'appliance répond avec succès à la demande de suppression, le sujet et les certificats Kafka de l'appliance sont supprimés.

Note La mise hors service d'une appliance ne peut pas être annulée. Pour restaurer l'appliance et les connecteurs, une nouvelle appliance doit être déployée et les connecteurs doivent être activés sur cette dernière.

Surveillance d'une appliance virtuelle

Les appliances virtuelles Cisco Secure Workload envoient régulièrement des signaux de présence et des statistiques à Cisco Secure Workload. L'intervalle du signal de présence (heartbeat) est de 5 minutes. Les messages de signal de présence heartbeat comprennent des statistiques sur l'intégrité de l'appliance, notamment des statistiques du système, des statistiques de processus et des statistiques sur le nombre de messages envoyés, reçus ou erronés sur le sujet Kafka utilisé pour la gestion de l'appliance.

Toutes les métriques sont disponibles dans *Digger* (OpenTSDB) et sont étiquetées avec l'ID de l'appliance et le nom de la portée racine. En outre, les tableaux de bord Grafana pour le *contrôleur d'appliances* sont également disponibles pour les mesures importantes de l'appareil.

Questions de sécurité

Le système d'exploitation invité de la machine virtuelle d'acquisition/de périphérie est CentOS 7.9, dans la version logicielle de serveur/client OpenSSL qui a été supprimée. Par conséquent, la seule façon d'accéder à l'appareil est via sa console.

Note CentOS 7.9 est le système d'exploitation invité pour les appareils virtuels d'acquisition et de périphérie de Cisco Secure Workload 3.8.1.19 et les versions antérieures. À partir de la version 3.8.1.36 de Cisco Secure Workload, le système d'exploitation est AlmaLinux 9.2.

Les conteneurs exécutent une image Docker basée sur centos : 7.9.2009. La plupart des conteneurs sont exécutés avec les privilèges de base (option sans privilège), à l'exception du conteneur ERSPAN, qui a la capacité NET_ADMIN.

Note À partir de la version 3.8.1.36 de Cisco Secure Workload, les conteneurs exécutent almalinux/9-base:9.2.

Dans le cas improbable où un conteneur serait contaminé, le système d'exploitation invité de la machine virtuelle ne devrait pas pouvoir être contaminé depuis l'intérieur du conteneur.

Gestion de la configuration sur les connecteurs et les appliances virtuelles

Les mises à jour de configuration peuvent être envoyées vers les appareils et les connecteurs à partir de Cisco Secure Workload. L'appareil doit s'être enregistré avec succès auprès de Cisco Secure Workload et être *actif* avant que les mises à jour de configuration puissent être lancées. De même, les connecteurs doivent être enregistrés auprès de Cisco Secure Workload avant que les mises à jour de configuration puissent être lancées sur leurs services.

Trois modes de mise à jour de la configuration sont possibles dans les appareils et les connecteurs.

1. **Test and Apply** (Tester et appliquer) : testez la configuration et, si le test est réussi, validez-la.
2. **Discovery** (Découverte) : testez la configuration et, si le test est réussi, découvrez les propriétés supplémentaires qui peuvent être activées pour la configuration.
3. **Remove** (Supprimer) : supprimer la configuration.

Note L'appareil et le connecteur ERSPAN ne prennent pas en charge les mises à jour de configuration.

Tester et appliquer

Les configurations qui prennent en charge le mode *Test and Apply* (Tester-Appliquer) vérifient la configuration avant d'appliquer (valider) la configuration sur l'appareil et/ou le connecteur souhaité.

Configuration du protocole NTP

La configuration NTP permet à l'appareil de synchroniser l'horloge avec le ou les serveurs NTP précisés.

Nom du paramètre	Type	Description
Activer NTP	case	La synchronisation NTP doit-elle être activée?
Serveurs NTP	listof chaînes	Liste des serveurs NTP Au moins un serveur doit être indiqué et un maximum de cinq serveurs peuvent être fournis.

Test (Tester) : tester si une connexion UDP peut être établie avec les serveurs NTP donnés sur le port 123. Si une erreur se produit pour l'un des serveurs NTP, n'acceptez pas la configuration.

Apply (Appliquer) : mettez à jour `/etc/ntp.conf` et redémarrez le service ntpd à l'aide de systemctl restart ntpd.service. Voici le modèle pour générer le fichier *ntp.conf*

```
# --- GENERAL CONFIGURATION ---
server <ntp-server>
...
server 127.127.1.0
fudge 127.127.1.0 stratum 10
# Drift file
driftfile /etc/ntp/drift
```

Note Applicable à Cisco Secure Workload 3.8.1.19 et aux versions antérieures.

Pour Cisco Secure Workload 3.8.1.36 ou une version ultérieure, mettez à jour `/etc/chrony.conf` et redémarrez le service chronyd à l'aide de systemctl restart chronyd.service. Voici le modèle pour générer le fichier *chrony.conf*

```
# Secure Workload appliance chrony.conf.
server <ntp-server> iburst
...
driftfile /var/lin/chrony/drift
makestep 1.0 3
rtcsync
```

Appliances virtuelles Cisco Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 134: Erreur lors du test de la configuration NTP

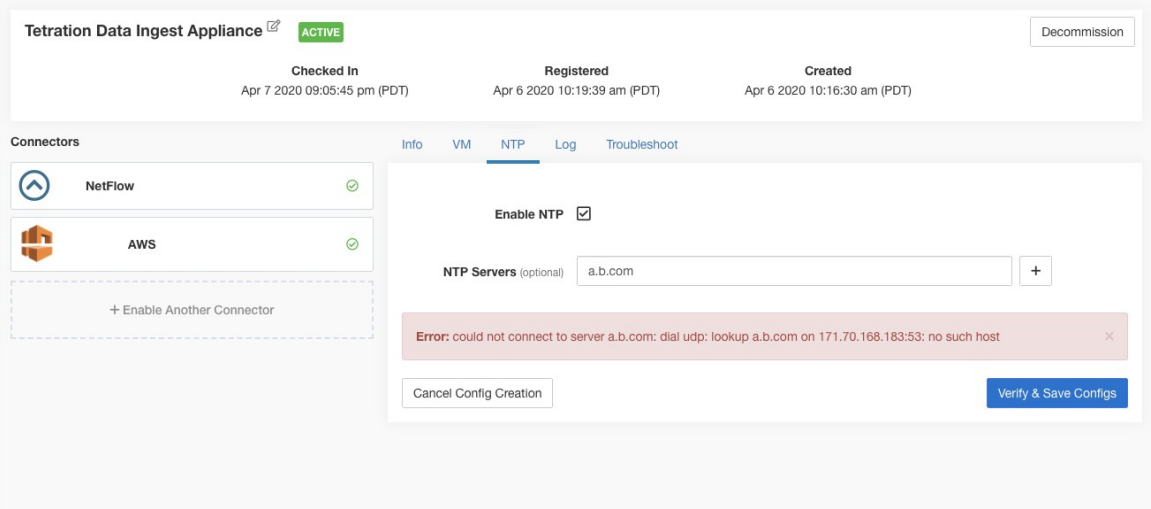


Figure 135: Configuration NTP avec des serveurs NTP valides

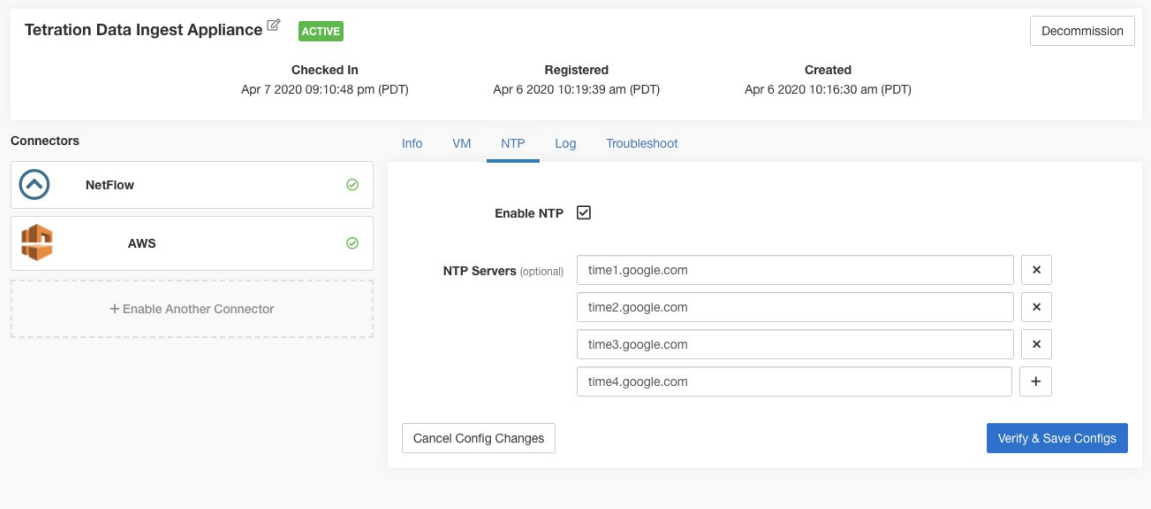
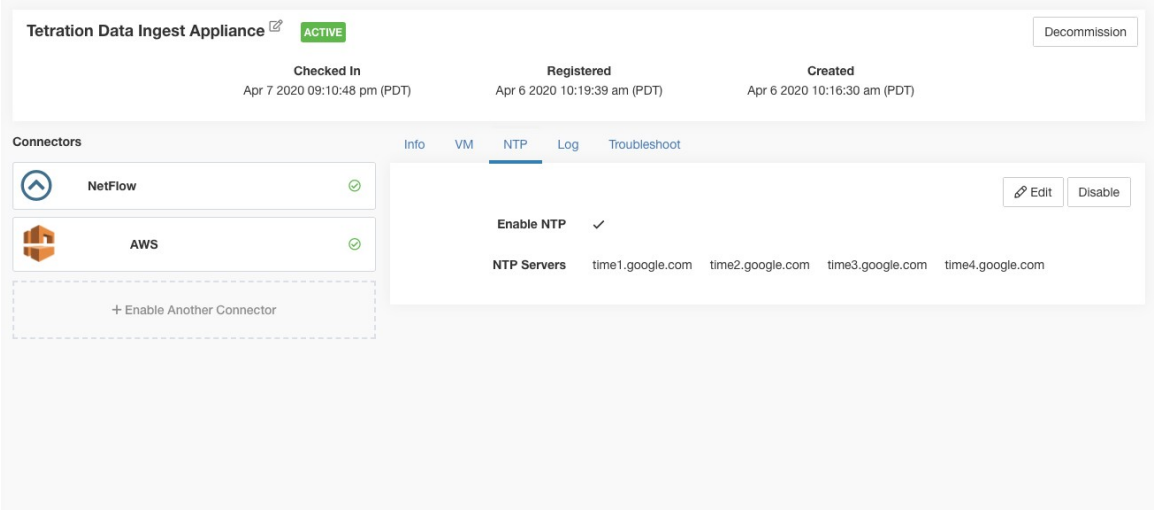


Figure 136: Configuration NTP vérifiée et appliquée



Configuration de la journalisation

La configuration des journaux met à jour les niveaux de journalisation, la taille maximale des fichiers journaux et les paramètres de rotation des journaux sur l'appareil et/ou le connecteur. Si la mise à jour de la configuration est déclenchée sur l'appareil, les paramètres du journal du contrôleur de l'appareil sont mis à jour. En revanche, si la mise à jour de la configuration est déclenchée sur un connecteur, les paramètres du contrôleur et du journal de service sont mis à jour.

Nom du paramètre	Type	Description
Niveau de journalisation	liste déroulante	Niveau de journalisation à définir
	• *débogage*	Niveau de journal de débogage
	• *Information*	Niveau de journalisation informatif
	• *avertir*	Niveau du journal des avertissements
	• *erreur*	Niveau du journal des erreurs
Taille maximale du fichier journal (en Mo)	number	Taille maximale d'un fichier de journal avant le début de la rotation des journaux
Rotation des journaux (en jours)	number	Longévité maximale d'un fichier journal avant le début de la rotation des journaux
Rotation des journaux (dans les instances)	number	Nombre maximal d'instances de fichiers journaux conservées

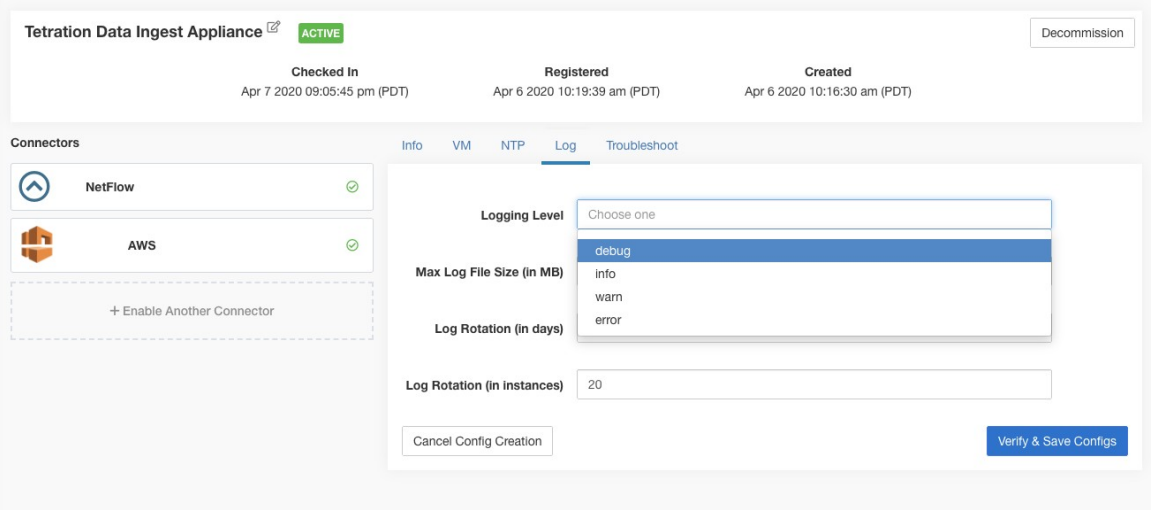
Test : pas d'opération

Apply (Appliquer) : Si la configuration est déclenchée sur un appareil, mettez à jour le fichier de configuration de *tet-controller* sur l'appareil. Si la configuration est déclenchée sur un connecteur, mettez à jour les fichiers de configuration de *tet-controller* et le service géré par le contrôleur sur le conteneur Docker responsable du connecteur.

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, ISE, ASA et Meraki.

Figure 137: Configurer le journal sur l'appareil



Note Comme tous les connecteurs de notification d'alerte (Syslog, Courriel, Slack, PagerDuty et Kinesis) fonctionnent sur un seul service Docker (Secure Workload Alert Alert Notifier) sur Cisco Secure Workload Edge, il n'est pas possible de mettre à jour la configuration du journal d'un connecteur sans avoir une incidence sur la configuration d'un autre connecteur de notification d'alerte. Les configurations des journaux du service Docker Cisco Secure Workload Alert Notifier (TAN) sur l'appareil de périphérie Cisco Secure Workload peuvent être mises à jour à l'aide d'une commande autorisée.

Consultez la section Mettre à jour la configuration des journaux du connecteur de l'outil de notification d'alerte pour de plus amples renseignements.

Configuration du point terminal

La configuration de point terminal précise le délai d'inactivité des points terminaux sur les connecteurs AnyConnect et ISE. Lorsqu'un point terminal expire, le connecteur arrête de s'enregistrer auprès de Cisco Secure Workload et purge l'état local du point terminal sur le connecteur.

Nom du paramètre	Type	Description
Délai d'expiration d'inactivité pour les points terminaux (en minutes)	number	Délai d'inactivité pour les points terminaux publiés par les connecteurs AnyConnect et ISE. À l'expiration du délai, le point terminal ne procédera plus à l'enregistrement de Cisco Secure Workload. (Valeur par défaut : 30 minutes).

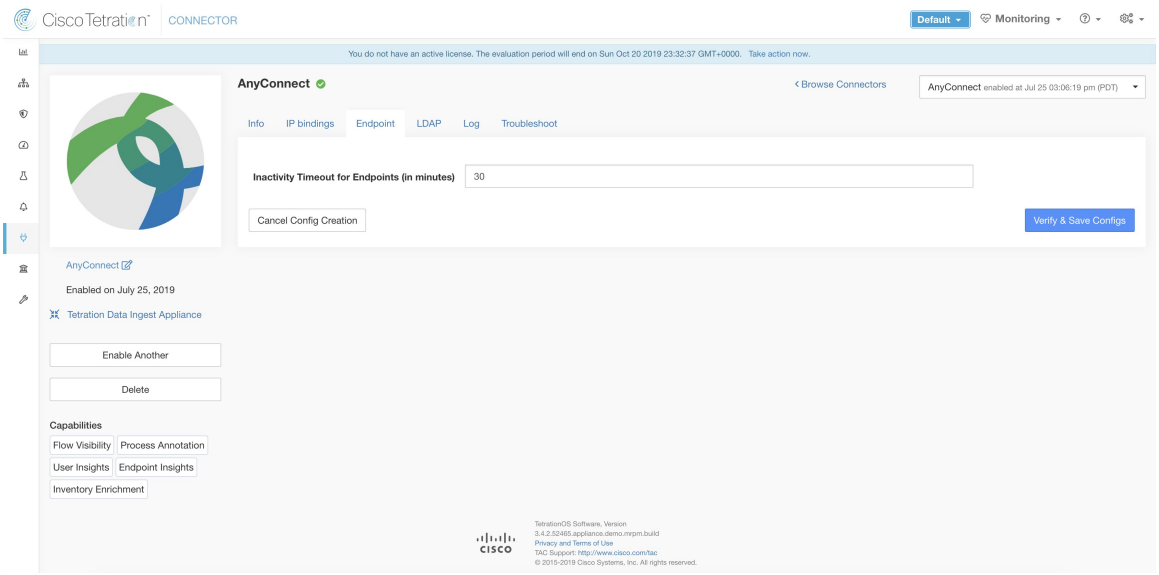
Test : pas d'opération

Apply (Appliquer) : mettez à jour le fichier de configuration du connecteur avec la nouvelle valeur

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : AnyConnect et ISE

Figure 138: Configuration du délai d'inactivité des points terminaux sur le connecteur AnyConnect



Configuration de l'outil de notification Slack

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur Slack.

Nom du paramètre	Type	Description
URL de point d'ancrage Web Slack	chaîne	Point d'ancrage Web Slack sur lequel les alertes Cisco Secure Workload doivent être publiées

Test(Tester) : envoyez une alerte de test à Slack à l'aide du point d'ancrage Web. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : Slack

Configuration de l'outil de notification PagerDuty

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur PagerDuty.

Nom du paramètre	Type	Description
Clé de service PagerDuty	chaîne	Clé de service PagerDuty pour l'envoi des alertes de Cisco Secure Workload sur PagerDuty

Test : permet d'envoyer une alerte de test à PagerDuty à l'aide de la clé de service. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : PagerDuty

Configuration de l'outil de notification Kinesis

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur Amazon Kinesis.

Nom du paramètre	Type	Description
ID de la clé d'accès AWS	chaîne	ID de clé d'accès AWS pour communiquer avec AWS
Clé d'accès secrète AWS	chaîne	Clé d'accès secrète AWS pour communiquer avec AWS
Région AWS	dropdown of AWS regions	Nom de la région AWS où le flux Kinesis est configuré
Kinesis Stream	chaîne	Nom du flux Kinesis
Stream Partition	chaîne	Nom de la partition du flux

Test (Tester) : envoie une alerte de test au flux Kinesis en utilisant la configuration donnée. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : Kinesis

Configuration de l'outil de notification des courriels

Configuration par défaut pour la publication des alertes Cisco Secure Workload dans un courriel.

Nom du paramètre	Type	Description
Nom d'utilisateur SMTP	chaîne	Nom d'utilisateur du serveur SMTP Ce paramètre est facultatif.
Mot de passe SMTP	chaîne	Mot de passe du serveur SMTP pour l'utilisateur (si fourni) Ce paramètre est facultatif.
SMTP Server	chaîne	Nom d'hôte ou adresse IP du serveur SMTP
Port SMTP	number	Port d'écoute du serveur SMTP. La valeur par défaut est 587.
Connection sécurisée	case	Doit-on utiliser SSL pour la connexion au serveur SMTP?
Adresse courriel d'expédition	chaîne	Adresse courriel à utiliser pour l'envoi des alertes
Destinataires par défaut	chaîne	Liste d'adresses courriel de destinataires séparées par des virgules

Test : envoyez un courriel de test en utilisant la configuration fournie. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : courriel

Configuration de l'outil de notification Syslog

Configuration par défaut pour la publication des alertes Cisco Secure Workload dans Syslog.

Nom du paramètre	Type	Description
Protocol	liste déroulante	Protocole à utiliser pour la connexion au serveur
	•*UDP*	
	• *TCP*	
Adresse du serveur	chaîne	Nom d'hôte ou adresse IP du serveur Syslog.
Port	number	Port d'écoute du serveur Syslog. La valeur du port par défaut est 514.

Test (Tester): envoie une alerte de test au serveur Syslog en utilisant la configuration donnée. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : syslog

Configuration du mappage de gravité Syslog

Le tableau suivant présente le mappage de gravité par défaut pour les alertes Cisco Secure Workload dans Syslog.

Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
FAIBLE	LOG_DEBUG
MOYENNE	LOG_WARNING
ÉLEVÉE	LOG_ERR
CRITIQUE	JOURNAL_CRIT
ACTION IMMÉDIATE	LOG_EMERG

Vous pouvez modifier ce paramètre à l'aide de cette configuration.

Nom du paramètre	Liste déroulante des mappages
ACTION_IMMÉDIATE	• *Urgence* • *Alerte* • *Critique* • *Erreur* • *Avertissement* • *Avis* • *Information* • *Débogage*
CRITIQUE	
ÉLEVÉ	
MOYENNE	
FAIBLE	

Test : pas d'opération

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : syslog

Configuration de l'instance ISE

Cette configuration fournit les paramètres nécessaires pour la connexion à Cisco Identity Services Engine (ISE). En fournissant plusieurs instances de cette configuration, le connecteur ISE peut se connecter et extraire les métadonnées concernant les points terminaux de plusieurs appareils ISE. Jusqu'à 20 instances de configuration ISE peuvent être fournies.

Nom du paramètre	Type	Description
Certificat client ISE	chaîne	Certificat client ISE pour se connecter à ISE à l'aide de pxGrid
Clé de client ISE	chaîne	Clé client ISE pour se connecter à ISE
Certificat de l'autorité de certification du serveur ISE	chaîne	Certificat de l'autorité de certification ISE
Nom d'hôte ISE	chaîne	Nom de domaine complet de ISE pxGrid
Nom de nœud ISE	chaîne	Nom de nœud de ISE pxGrid

Test (Test) : connectez-vous à ISE en utilisant les paramètres fournis. Une fois la connexion réussie, acceptez la configuration.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : ISE

Découverte

Les configurations qui prennent en charge le mode *découverte* effectuent ce qui suit.

1. Obtenir une configuration de base auprès de l'utilisateur.
2. Vérifier configuration de base.
3. Détecter les propriétés supplémentaires de la configuration et les présenter à l'utilisateur.
4. Laissez l'utilisateur améliorer la configuration à l'aide des propriétés découvertes.
5. Vérifier et appliquer la configuration améliorée.

Dans la version 3.3.1.x, la configuration LDAP prend en charge le mode de découverte.

Configuration LDAP

La configuration LDAP précise comment se connecter au LDAP, quel est le nom distinctif (DN) de base à utiliser, quel est l'attribut qui correspond au nom d'utilisateur et quels attributs récupérer pour chaque nom d'utilisateur. Les attributs LDAP sont des propriétés de LDAP qui sont spécifiques à cet environnement.

Compte tenu de la configuration de la connexion à LDAP et du DN de base, il est possible de découvrir les attributs des utilisateurs dans LDAP. Ces attributs détectés peuvent ensuite être présentés à l'utilisateur dans l'interface utilisateur. Parmi ces attributs découverts, l'utilisateur sélectionne l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à collecter pour chaque nom d'utilisateur à partir de LDAP. Par conséquent, cela rend inutile la configuration manuelle des attributs LDAP et réduit les erreurs.

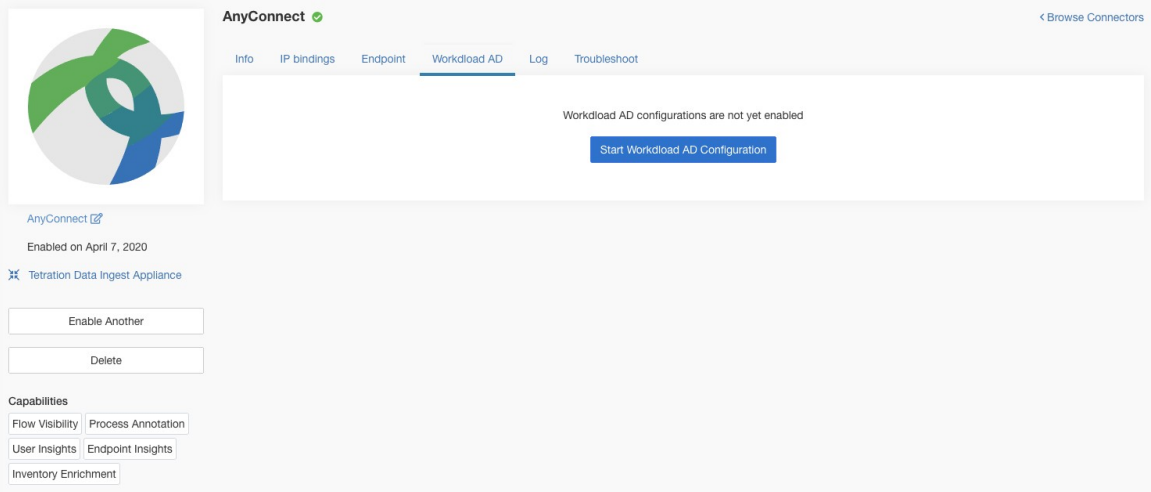
Voici les étapes détaillées de la création d'une configuration LDAP par découverte.

Procedure

Étape 1 Commencez la configuration LDAP

Lancez une configuration LDAP pour le connecteur.

Figure 139: Démarrez la découverte de la configuration LDAP



Étape 2 Fournissez une configuration LDAP de base

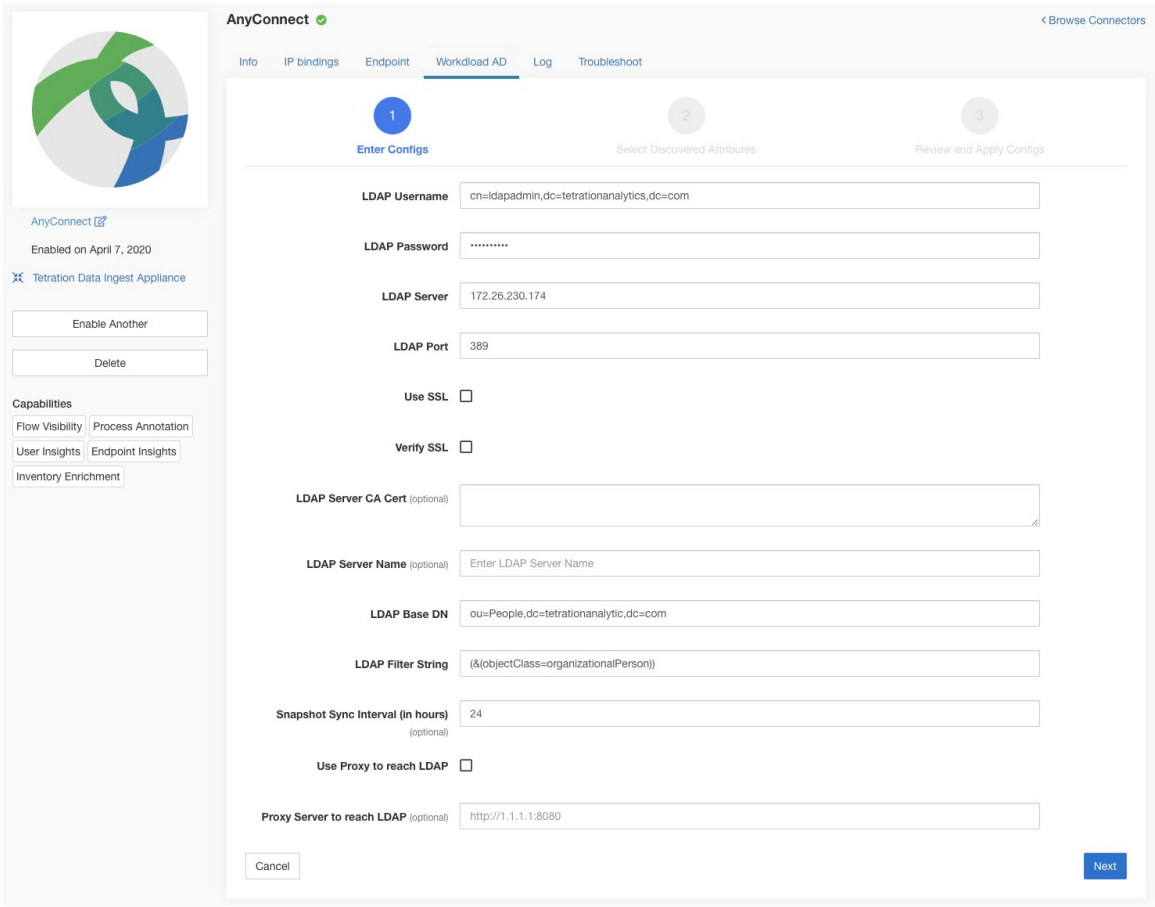
Précisez la configuration de base pour la connexion à LDAP. Dans cette configuration, les utilisateurs fournissent le DN de liaison LDAP ou le nom d'utilisateur pour la connexion au serveur LDAP, le mot de passe LDAP à utiliser pour la connexion au serveur LDAP, l'adresse du serveur LDAP, le port du serveur LDAP, le DN de base auquel se connecter et une chaîne de filtre pour récupérer les utilisateurs qui correspondent à ce fichier.

Nom du paramètre	Type	Description
Nom d'utilisateur LDAP	chaîne	Nom d'utilisateur LDAP ou DN de liaison pour accéder au serveur LDAP*
LDAP Password	chaîne	Mot de passe LDAP pour le nom d'utilisateur pour accéder au serveur LDAP*
LDAP Server	chaîne	Adresse du serveur LDAP
Port LDAP	number	Port du serveur LDAP
Utiliser le protocole SSL	case	Le connecteur doit-il se connecter à LDAP de manière sécurisée? Facultatif. La valeur par défaut est False.

Nom du paramètre	Type	Description
Verify SSL	case	Le connecteur doit-il vérifier le certificat LDAP? Facultatif. La valeur par défaut est False.
LDAP Server CA Cert	chaîne	Certificat de l'autorité de certification du serveur Facultatif.
Nom du serveur LDAP	chaîne	Nom du serveur pour lequel le certificat LDAP est émis (obligatoire si la case *Vérifier SSL* est cochée.
DN de base LDAP	chaîne	DN de base LDAP, le point de départ des recherches dans l'annuaire dans LDAP
LDAP Filter String	chaîne	Chaîne de préfixe de filtre LDAP Filtrez les résultats de la recherche qui correspondent uniquement à cette condition.
Snapshot Sync Interval (in hours)	number	Spécifiez l'intervalle de temps en heures pour (re)créer un instantané LDAP. Facultatif. Le réglage par défaut est de 24 heures.
Utiliser un serveur mandataire pour accéder à LDAP	case	Le connecteur doit-il utiliser un serveur mandataire pour accéder au serveur LDAP?
Serveur mandataire pour accéder à LDAP	chaîne	Serveur serveur mandataire pour accéder à LDAP

Les autorisations utilisateur minimales nécessaires pour configurer LDAP sur les connecteurs sont un **Utilisateur de domaine standard**.

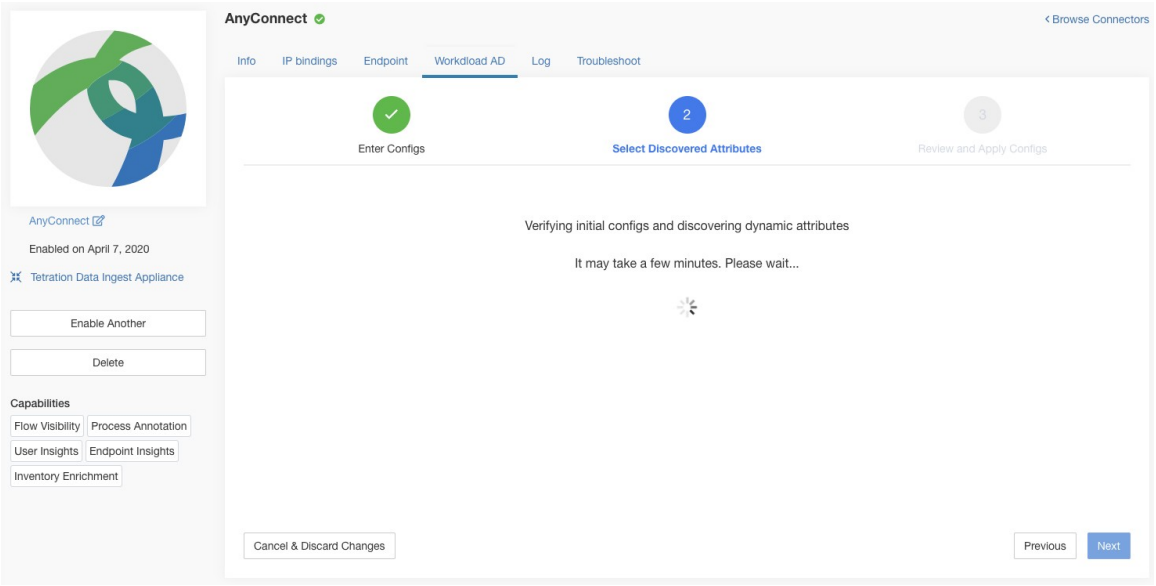
Figure 140: Configuration initiale LDAP



Étape 3 Découverte en cours

Une fois que l'utilisateur a cliqué sur *Next* (suivant), cette configuration est envoyée au connecteur. Le connecteur établit une connexion avec le serveur LDAP en utilisant la configuration fournie. Il récupère jusqu'à 1 000 utilisateurs du serveur LDAP et identifie tous les attributs. En outre, il calcule une liste de tous les attributs à valeur unique communs aux 1 000 utilisateurs. Le connecteur renvoie ce résultat à Cisco Secure Workload.

Figure 141: Découverte en cours



Étape 4 **Améliorez la configuration avec les attributs découverts**

L'utilisateur doit choisir l'attribut correspondant au nom d'utilisateur et sélectionner jusqu'à six attributs que le connecteur doit récupérer et enregistrer pour chaque utilisateur de de l'organisation (c'est-à-dire les utilisateurs correspondant à la chaîne de filtrage). Cette action est effectuée à l'aide d'une liste déroulante d'attributs détectés. Ainsi, vous éliminez les erreurs manuelles et les erreurs de configuration.

Nom du paramètre	Type	Description
Attribut de nom d'utilisateur LDAP	chaîne	Attribut LDAP qui contient le nom d'utilisateur
Attributs LDAP à récupérer	liste de chaînes	Liste des attributs LDAP qui doivent être extraits pour un utilisateur

Figure 142: Détecter les attributs LDAP

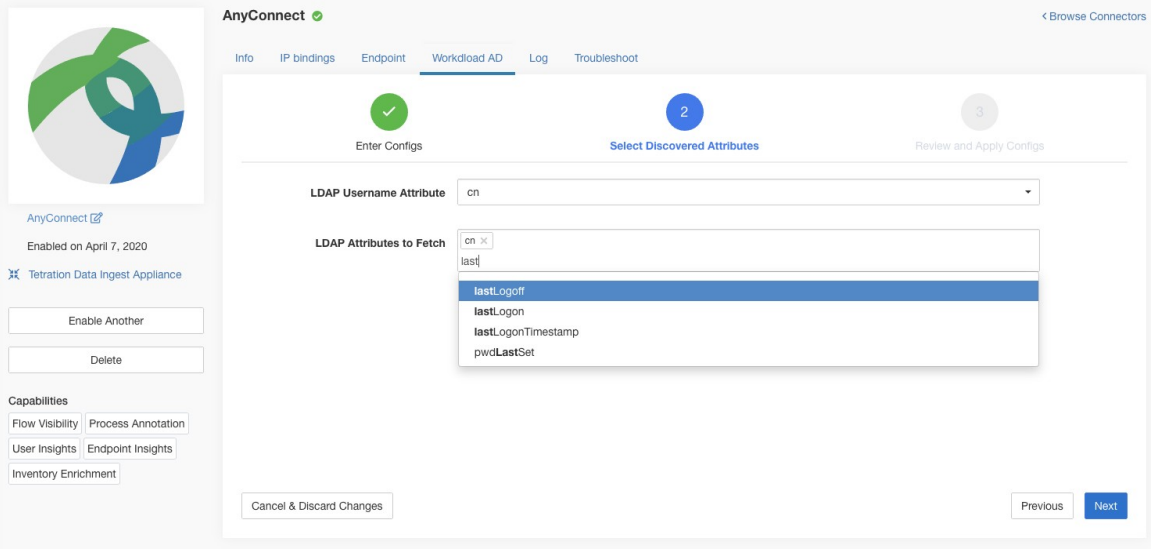
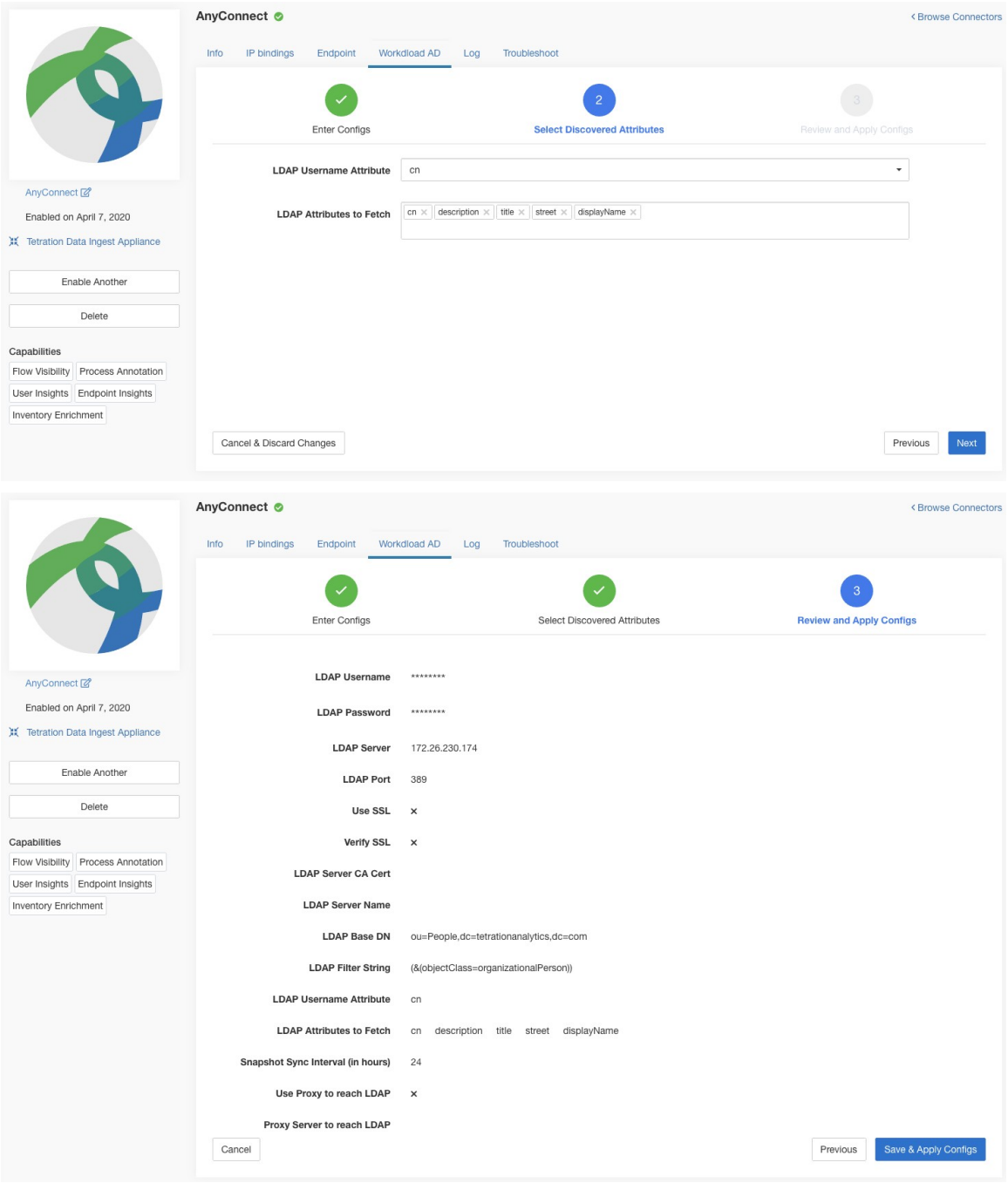


Figure 143: Déterminer l'attribut de nom d'utilisateur et les attributs à recueillir pour chaque nom d'utilisateur

Étape 5 Finaliser, enregistrer et appliquer la configuration

Enfin, la configuration est terminée en cliquant sur *Save and Apply Changes*(enregistrer et appliquer les modifications).

Figure 144: Terminer la découverte et la validation de la configuration LDAP



Le connecteur reçoit la configuration terminée. Il crée un instantané local de tous les utilisateurs correspondant à la chaîne de filtre et récupère uniquement les attributs sélectionnés. Une fois la prise d'instantané terminée, les services du connecteur peuvent commencer à utiliser l'instantané pour annoter les utilisateurs et leurs attributs LDAP dans les inventaires.

Appliances virtuelles Cisco Secure Workload autorisées : Aucune

Connecteurs autorisés : AnyConnect, ISE et F5.

Supprimer

Vous pouvez supprimer toutes les configurations que vous avez ajoutées des connecteurs ou des appareils en utilisant le bouton *Delete* (Supprimer) disponible pour chaque configuration.

Dépannage

Les connecteurs et les appliances virtuelles prennent en charge divers mécanismes de dépannage pour déboguer les problèmes éventuels.

Note La présente section ne s'applique pas aux éléments suivants :

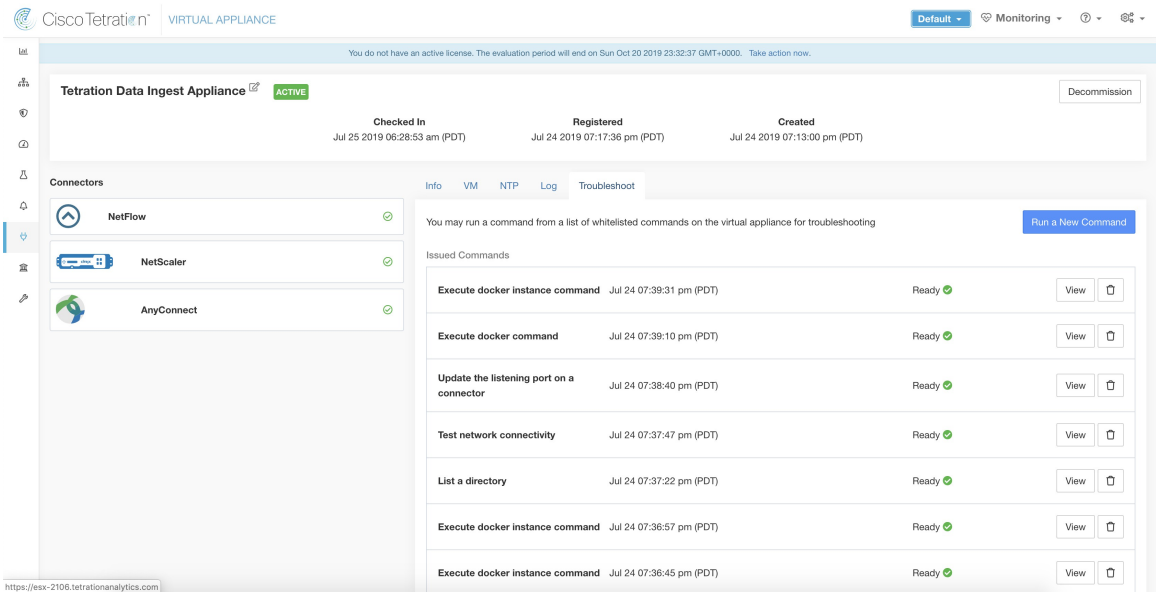
Appliance virtuelle ERSPAN : reportez-vous à la page de l'appliance ERSPAN pour en savoir plus sur le dépannage.

Connecteurs infonuagiques : pour dépanner les connecteurs infonuagiques, consultez la section de votre connecteur infonuagique, par exemple Résoudre les problèmes de connecteur AWS.

Ensemble de commandes autorisé

L'ensemble de commandes autorisé vous permet d'exécuter certaines commandes de débogage sur les appareils et les conteneurs Docker (pour les connecteurs). Les commandes autorisées comprennent la possibilité de récupérer les journaux et la configuration d'exécution actuelle, de tester la connectivité réseau et de capturer des paquets correspondant à un port spécifié.

Figure 145: Page de dépannage sur l'appliance virtuelle Cisco Secure Workload



Note Le dépannage à l'aide de l'ensemble de commandes autorisé est disponible sur les périphériques et les connecteurs uniquement pour les utilisateurs ayant le rôle *Service à la clientèle*.

Afficher les journaux

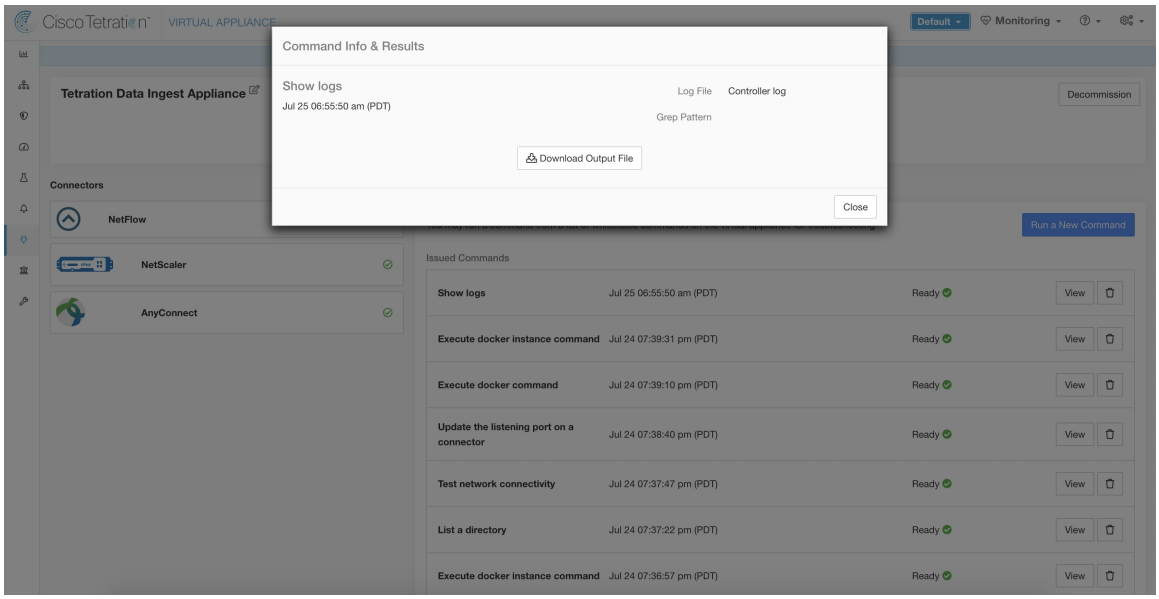
Affiche le contenu d'un fichier journal de contrôleur et permet éventuellement de traiter le fichier selon un modèle précisé. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Lorsque le résultat est disponible dans Cisco Secure Workload, un bouton de téléchargement s'affiche permettant de télécharger le fichier.

Nom de l'argument	Type	Description
Modèle Grep	chaîne	Chaîne de schéma Grep dans le fichier journal

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 146: Télécharger la sortie d'affichage des journaux à partir de l'appareil d'acquisition Cisco Secure Workload



Afficher les journaux de service

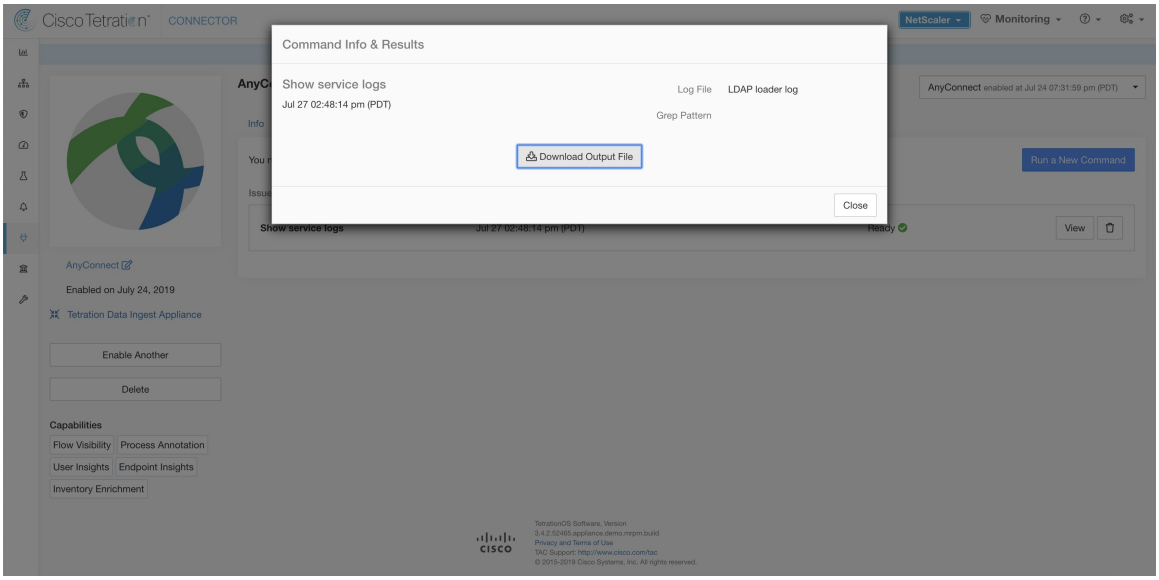
Affiche le contenu des fichiers journaux de service et permet éventuellement de saisir le fichier selon un modèle spécifié. Cisco Secure Workload envoie la commande à l'appareil/au connecteur sur lequel la commande a été exécutée. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Lorsque le résultat est disponible dans Cisco Secure Workload, un bouton de téléchargement s'affiche permettant de télécharger le fichier.

Nom de l'argument	Type	Description
Log File	liste déroulante	Le nom du fichier journal à collecter
	• *Service log*	Journaux du service du connecteur
	• *Upgrade log*	Journaux de mise à niveau du service
	• *LDAP loader log*	Journaux de l'instantané LDAP pour les connecteurs pour lesquels LDAP est activé
Modèle Grep	chaîne	Chaîne de schéma Grep dans le fichier journal

Appliances virtuelles Cisco Secure Workload autorisées : aucune (disponible uniquement avec les services de connecteur valides)

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 147: Téléchargez la sortie d'affichage des journaux de service du connecteur AnyConnect pour le fichier de journalisation du chargeur LDAP



Afficher la configuration d'exécution

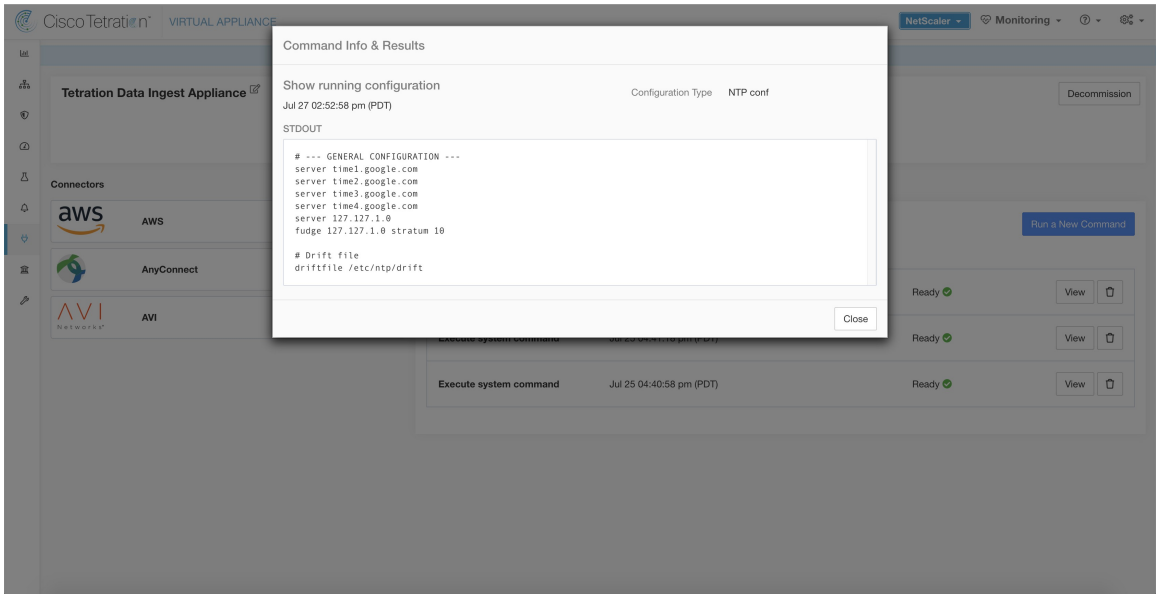
Afficher la configuration en cours d'exécution d'un appareil ou des contrôleurs de connecteur. Le contrôleur de l'appareil ou du connecteur récupère la configuration correspondant à l'argument demandé et renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, le contenu de la configuration s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Type de configuration	liste déroulante	Fichier de configuration à recueillir
	• *Configuration du contrôleur*	Fichier de configuration du contrôleur de l'appareil
	• *Configuration du superviseur*	Fichier de configuration du superviseur qui exécute le contrôleur
	• *Configuration NTP*	Fichier de configuration NTP
	• *Conférence Chrony*	/etc/chrony.conf

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 148: Afficher la configuration en cours d'exécution pour la conférence NTP sur un appareil d'acquisition Cisco Secure Workload



Afficher la configuration d'exécution du service

Affichez la configuration en cours d'exécution des services instanciés pour les connecteurs sur les appareils. Le contrôleur du service récupère la configuration correspondant à l'argument demandé et renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, le contenu de la configuration s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Type de configuration	liste déroulante	Fichier de configuration à recueillir.
	• *Configuration du contrôleur*	Fichier de configuration du contrôleur de service.
	• *Configuration du superviseur*	Fichier de configuration du superviseur qui exécute le contrôleur.
	• *Configuration de service*	Fichier de configuration du service.
	• *Configuration LDAP*	Configuration LDAP pour les connecteurs pour lesquels LDAP est activé.

Appliances virtuelles Cisco Secure Workload autorisées : aucune (disponible uniquement avec les services de connecteur valides)

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Afficher les commandes système

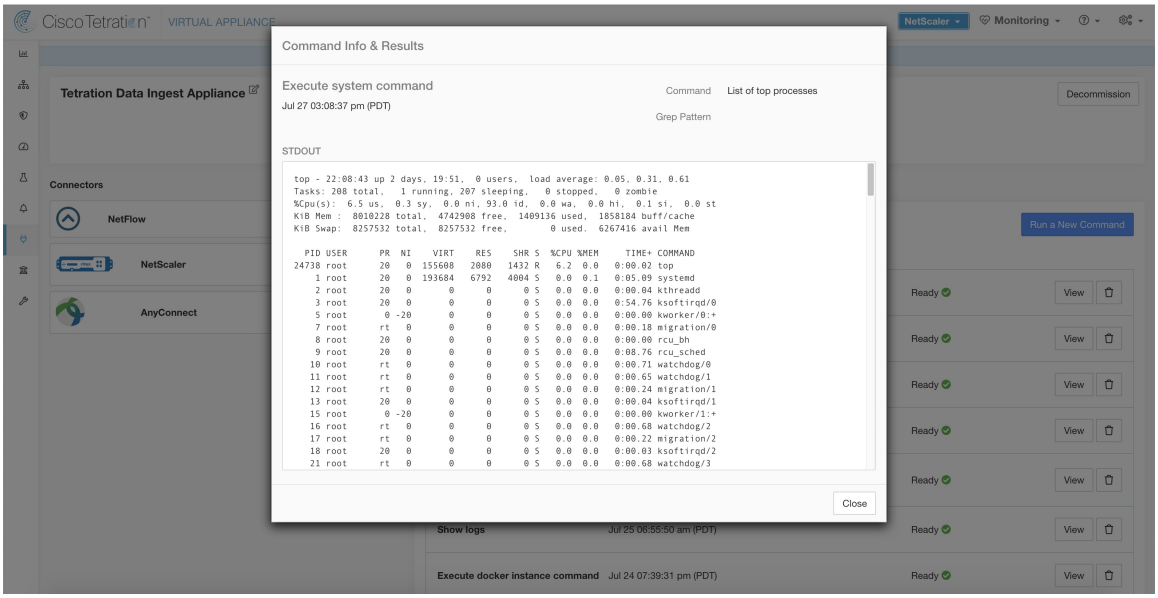
Exécutez une commande système et éventuellement grep pour un modèle spécifié. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commandes système	liste déroulante	Commande système à exécuter
	• *Configuration IP*	**ifconfig**
	• *Configuration de la route IP*	**ip route**
	• *Règles de filtrage de paquets IP*	**iptables -L**
	• *État du réseau*	**netstat**
	• *État du réseau (EL9)*	**ss**
	• *État du processus*	**ps -aux**
	• *Liste des principaux processus*	**top -b -n 1**
	• *État NTP*	**ntpstat**
	• *Requête NTP*	**ntpq -pn**
	• État Chrony (EL9)	**suivi Chronyc**
	• Requête Chrony (EL9)	**sources chronyc**
	• *Informations sur le processeur*	**lscpu**
	• *Informations sur la mémoire*	**lsmem**
	• *Disque libre*	**df -H**
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 149: Afficher la commande système sur l'appareil d'acquisition Cisco Secure Workload pour récupérer la liste des principaux processus



Afficher les commandes Docker

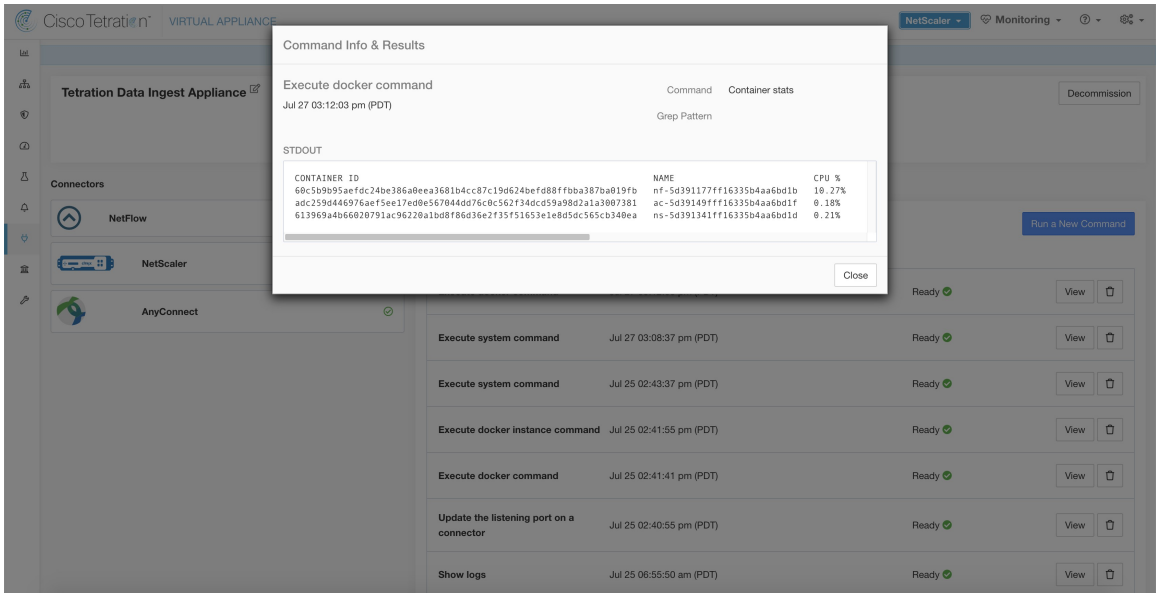
Exécutez une commande Docker et éventuellement grep pour un modèle spécifié. La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Le résultat s'est arrêté aux 5000 dernières lignes. Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande Docker	liste déroulante	Commande Docker à exécuter
	• *Docker info*	**Renseignements sur Docker**
	• *List images*	**images de Docker --non tronquées**
	• *List containers*	**Docker ps --non tronqués**
	• *List networks*	**réseau docker est --non tronqué**
	• *List volumes*	**volume Docker est**
	• *Statistiques des conteneurs*	**Statistiques de Docker –non tronquées - aucun flux**
	• *Utilisation du disque Docker*	`docker system df -v`
	• *Événements du système Docker*	**Événements système Docker --depuis '10m'**
	• *Version*	**version de Docker**
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 150: Exécutez une commande Docker sur l'appareil d'acquisition Cisco Secure Workload pour afficher les statistiques du conteneur



Afficher les commandes d'instance Docker

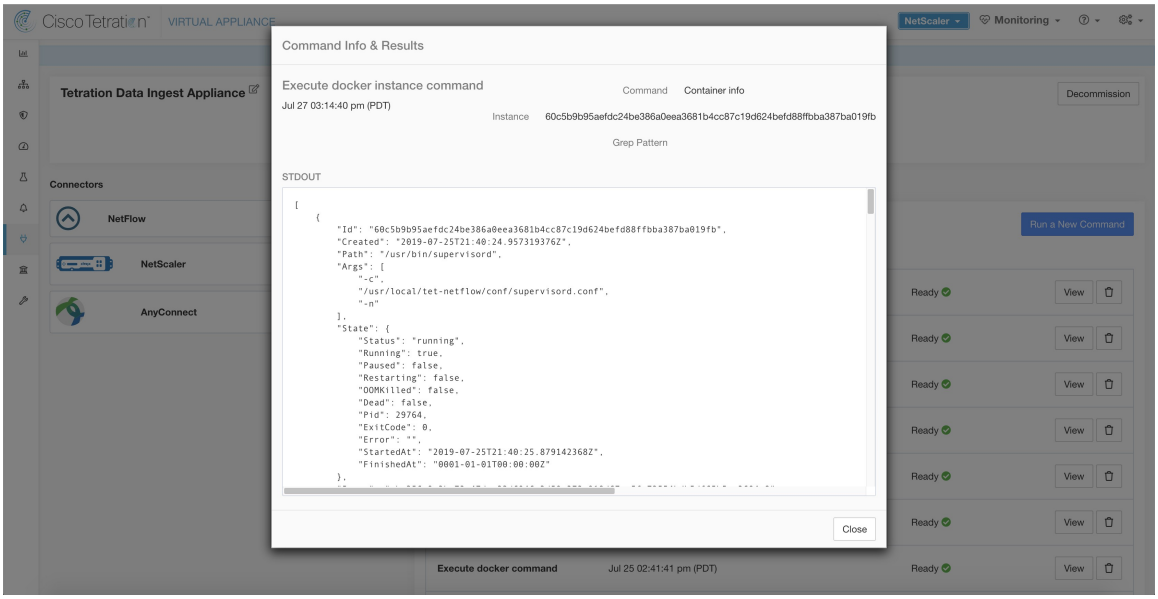
Exécutez une commande Docker sur une instance spécifique d'une ressource Docker. L'ID d'instance peut être récupéré à l'aide de l'option Afficher les commandes Docker (Afficher les commandes Docker). La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Le résultat s'est arrêté aux 5000 dernières lignes. Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande Docker	liste déroulante	Commande Docker à exécuter
	• *Informations sur l'image*	**images de Docker --non tronquées <instance>**
	• *Informations sur le réseau*	**inspection du réseau de Docker<instance>**
	• *Informations sur le volume*	**Inspecter le volume Docker<instance>**
	• *Informations sur le conteneur*	**Docker conteneur inspect--taille<instance>**
	• *Journaux des conteneurs*	**Journaux Docker --derniers 5000<instance>**
	• *Mappages de ports de conteneur*	**port Docker<instance>**
	• *Statistiques d'utilisation des ressources du conteneur*	**Statistiques Docker –non tronquée--aucun flux<instance>**
	• *Processus en cours d'exécution de conteneur*	**docker top <instance>**
Instance	chaîne	ID de ressource Docker (image, réseau, volume, conteneur) (voir Afficher les commandes Docker)
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 151: Exécutez une commande d'instance Docker sur l'appareil d'acquisition Cisco Secure Workload pour récupérer les informations sur le conteneur



Afficher les commandes du superviseur

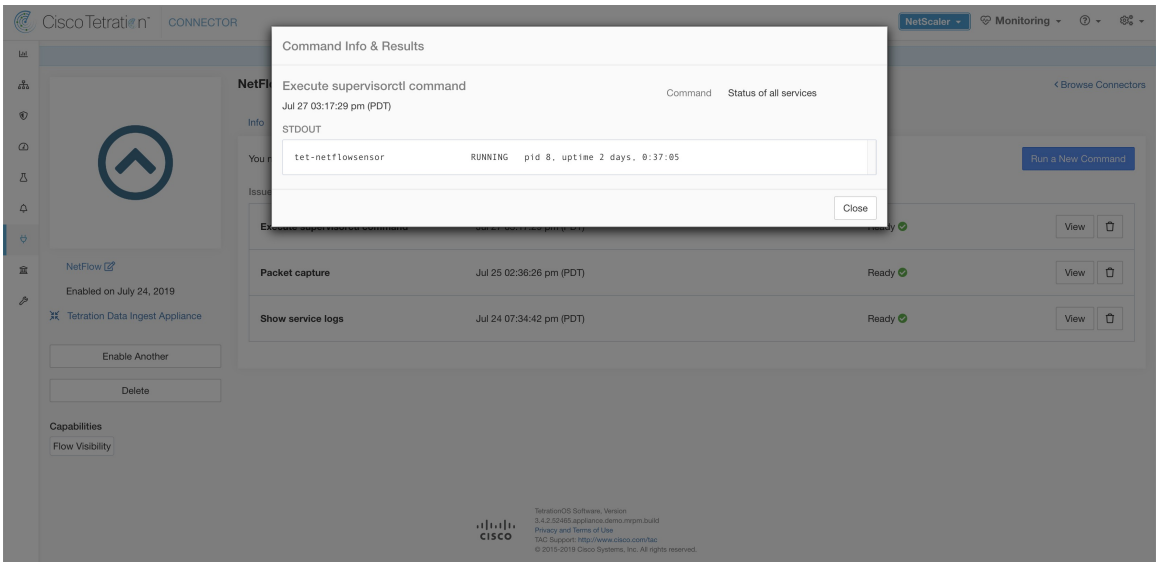
Exécutez une commande supervisorctl et renvoyez le résultat. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur sur le dispositif ou le service du connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Commande SupervisorCtl	liste déroulante	commande *supervisorctl* à exécuter
	• *État de tous les services*	**supervisorctl status**
	• *PID du superviseur*	**supervisorctl pid all**
	• *PID de tous les services*	**supervisorctl pid all**

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 152: Exécutez la commande supervisorctl sur le connecteur NetFlow pour obtenir l'état de tous les services

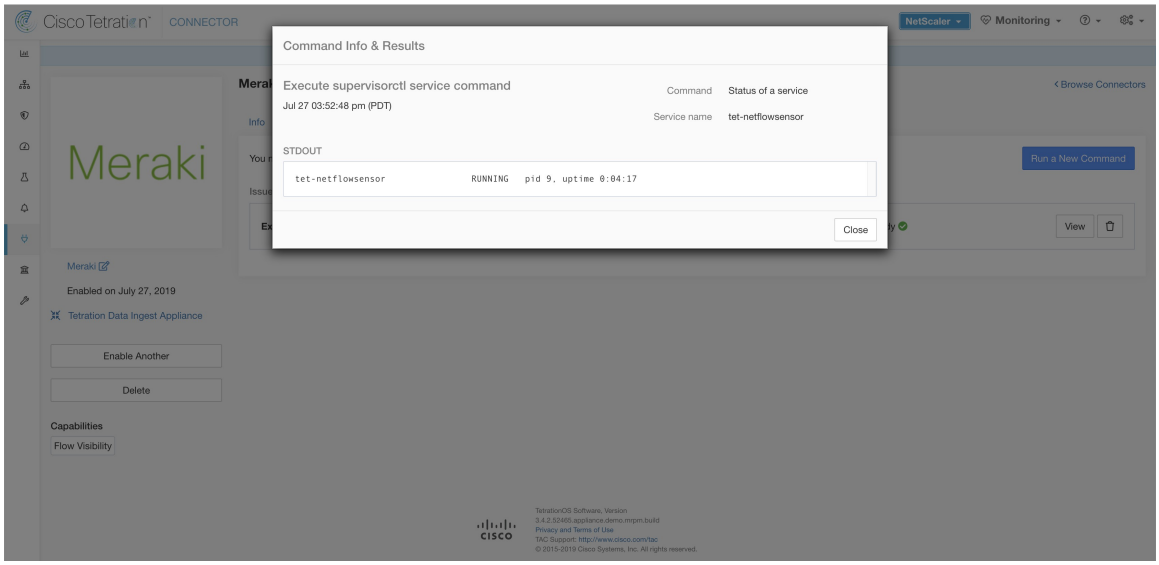


Afficher les commandes de service du superviseur

Exécutez une commande supervisorctl pour un service spécifique. Le nom du service peut être récupéré à l'aide Afficher les commandes du superviseur(afficher le superviseur). Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été émise. Le contrôleur service de l'appareil/du connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande SupervisorCtl	liste déroulante	commande *supervisorctl* à exécuter
	• *État d'un service*	**supervisorctl status <nom du service>**
	• *PID d'un service*	**supervisorctl pid <nom du service>**
Service name	chaîne	Nom du service contrôlé par le superviseur (voir la section Afficher les commandes du superviseur)

Figure 153: Exécutez la commande supervisorctl sur le connecteur NetFlow pour obtenir l'état du nom de service spécifié



Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Commandes de connectivité réseau

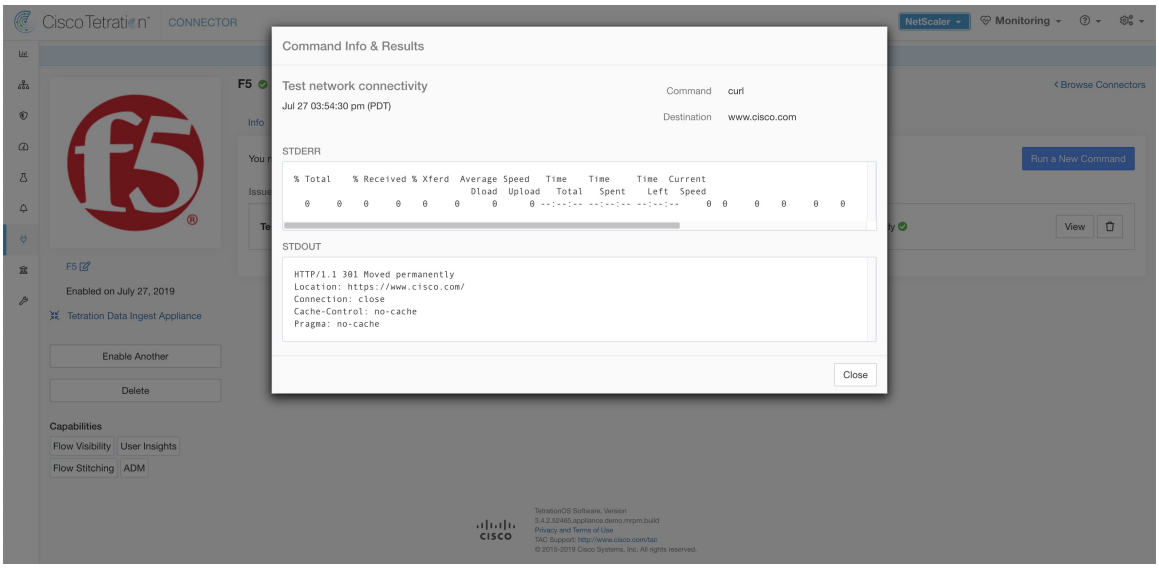
Tester la connectivité réseau à partir de l'appareil ou du connecteur. La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande réseau	liste déroulante	Commande de connectivité réseau à exécuter
	• *ping*	**ping -c 5 <destination>**
	• *boucle*	**curl -I <destination>**
Destination	chaîne	Destination à utiliser pour le test

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 154: Testez la connectivité réseau sur le connecteur F5 en exécutant une commande boucle



Répertorier les fichiers

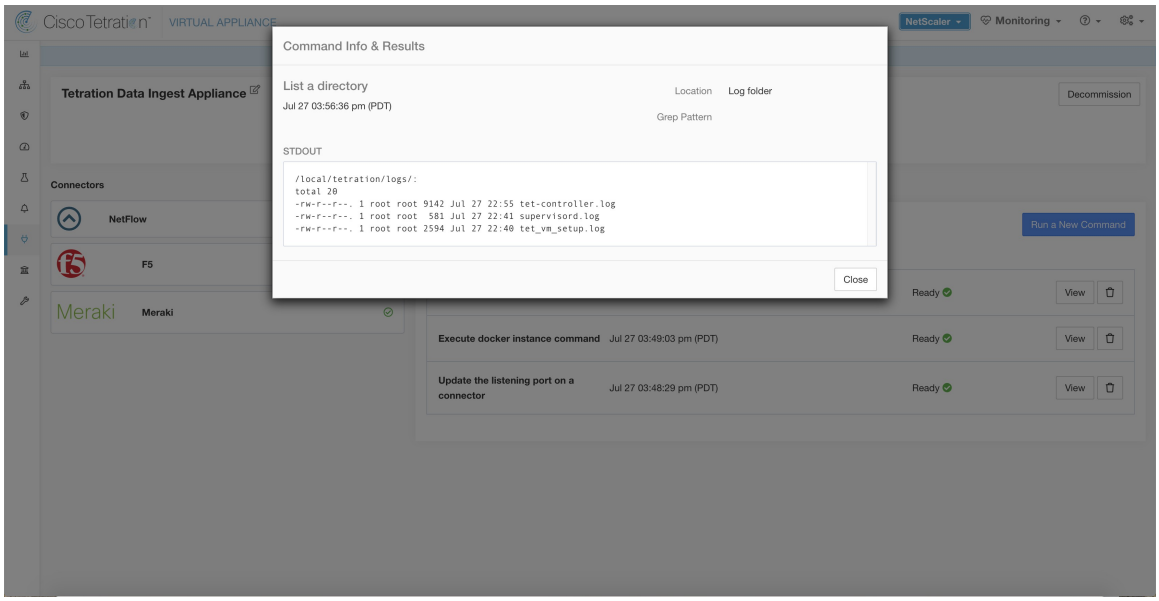
Répertoriez les fichiers dans les emplacements bien connus de l'appareil. Vous pouvez également utiliser la fonction grep pour un modèle spécifié. Cisco Secure Workload envoie la commande à l'appareil où la commande a été exécutée. Le contrôleur de l'appareil renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Site	liste déroulante	Répertorier les fichiers dans un emplacement cible
	• *Dossier de configuration du contrôleur*	Répertorie le contenu dans le dossier où sont conservés les fichiers de configuration du contrôleur.
	• *Dossier du certificat du contrôleur*	Répertorie le contenu dans le dossier où les certificats du contrôleur sont conservés.
	• *Dossier des journaux*	Répertorie le contenu dans le dossier où se trouvent les fichiers journaux.
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 155: Répertorier les fichiers du dossier journal de l'appareil d'acquisition Cisco Secure Workload



Répertorier les fichiers de service

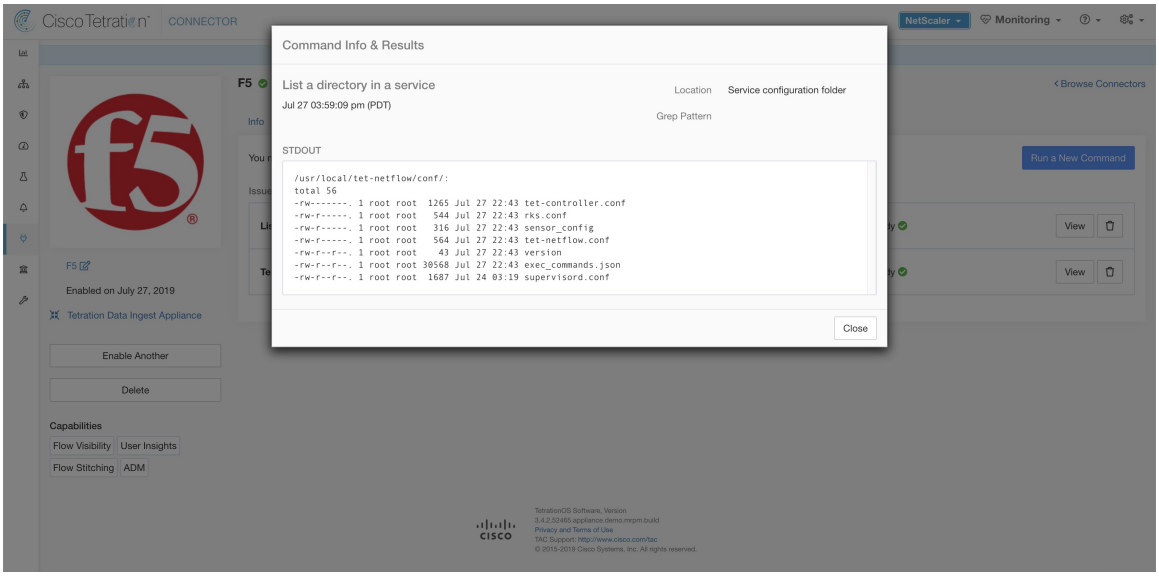
Répertoriez les fichiers dans les emplacements bien connus du service du connecteur. Vous pouvez également utiliser grep pour un modèle spécifié. Cisco Secure Workload envoie la commande au connecteur où la commande a été émise. Le contrôleur sur le service de connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Site	liste déroulante	Répertorier les fichiers dans un emplacement cible.
	• *Dossier de configuration du service*	Répertorie le contenu du dossier où les fichiers de configuration du service sont conservés.
	• *Dossier du certificat de service*	Répertorie le contenu du dossier où les certificats de service sont conservés.
	• *Dossier des journaux*	Répertorie le contenu dans le dossier où se trouvent les fichiers journaux.
	• *Dossier de base de données*	Répertorie le contenu du dossier où l'état des terminaux (en particulier pour les connecteurs AnyConnect et ISE) est conservé.
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 156: Répertorie les fichiers du dossier de configuration du connecteur F5 dans l'appareil d'acquisition Cisco Secure Workload



Capture de paquets

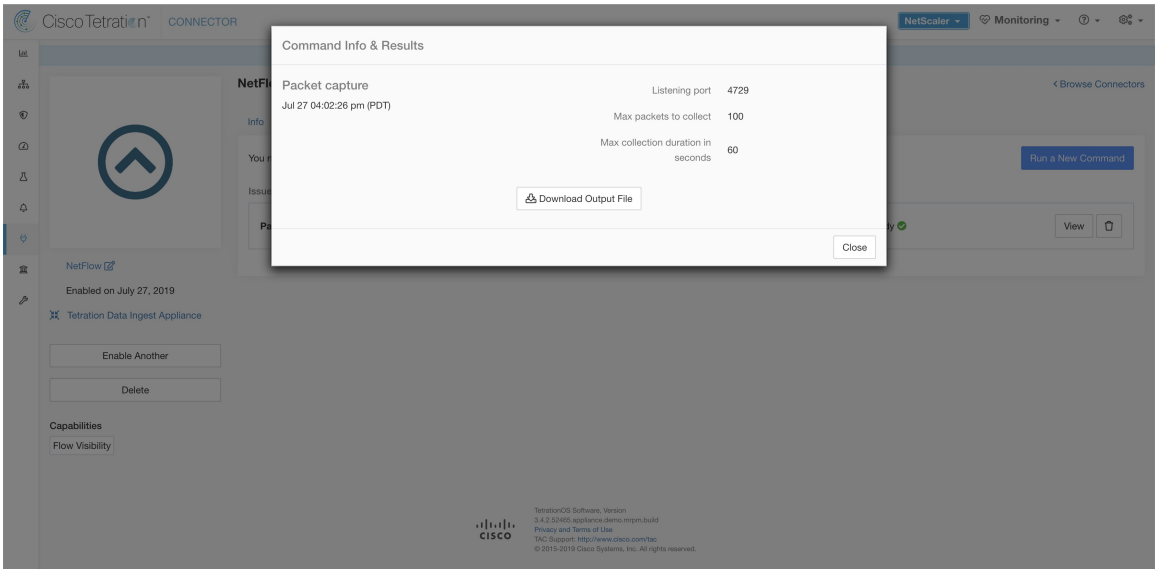
Capturer les paquets entrants sur un appareil ou un connecteur. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur du service de l'appareil ou du connecteur capture les paquets, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.pcap`.

Nom de l'argument	Type	Description
Port d'écoute	number	Capturer les paquets envoyés ou reçus sur ce port
Nombre maximal de paquets à collecter	number	Nombre maximal de paquets à collecter avant de renvoyer le résultat. Il doit être inférieur à 1000
Durée maximale de la collecte en secondes	number	Durée maximale à collecter avant de renvoyer le résultat. Elle doit être inférieure à 600 secondes.

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 157: Capturer des paquets sur un port donné du connecteur NetFlow



Mettre à jour les ports d'écoute des connecteurs

Mettez à jour le port d'écoute sur un connecteur dans le dispositif d'acquisition Cisco Secure Workload. Cisco Secure Workload envoie la commande au contrôleur de l'appareil sur l'appareil sur lequel la commande est exécutée. Le contrôleur effectue les actions suivantes :

- Arrête le service Docker correspondant au connecteur.
- Recueille la configuration d'exécution actuelle du service.
- Supprime le service Docker.
- Met à jour la configuration d'exécution du service pour utiliser les nouveaux ports.
- Démarre un nouveau conteneur à partir de la même image Docker que celle utilisée dans le conteneur supprimé, avec de nouveaux ports accessibles. De plus, si un volume Docker a été monté sur le conteneur supprimé précédemment, le même volume est monté sur le nouveau conteneur.
- Renvoie les nouvelles liaisons IP du connecteur à Cisco Secure Workload.
- Cisco Secure Workload affiche le résultat dans une zone de texte.

Nom de l'argument	Type	Description
ID du connecteur	chaîne	ID de connecteur du connecteur pour lequel les ports d'écoute doivent être mis à jour
Étiquette de port d'écoute	liste déroulante	Le type de port qui est mis à jour.
	NET-FLOW9	Port d'écoute NetFlow v9
	IPFIX	Port d'écoute IPFIX

Nom de l'argument	Type	Description
Port d'écoute	chaîne	Nouveau port pour le connecteur

Appliances virtuelles Secure Workload autorisées : acquisition Cisco Secure Workload

Connecteurs autorisés : aucun

Figure 158: Mettre à jour le port d'écoute sur le connecteur Meraki à 2055 dans l'appareil d'acquisition Cisco Secure Workload

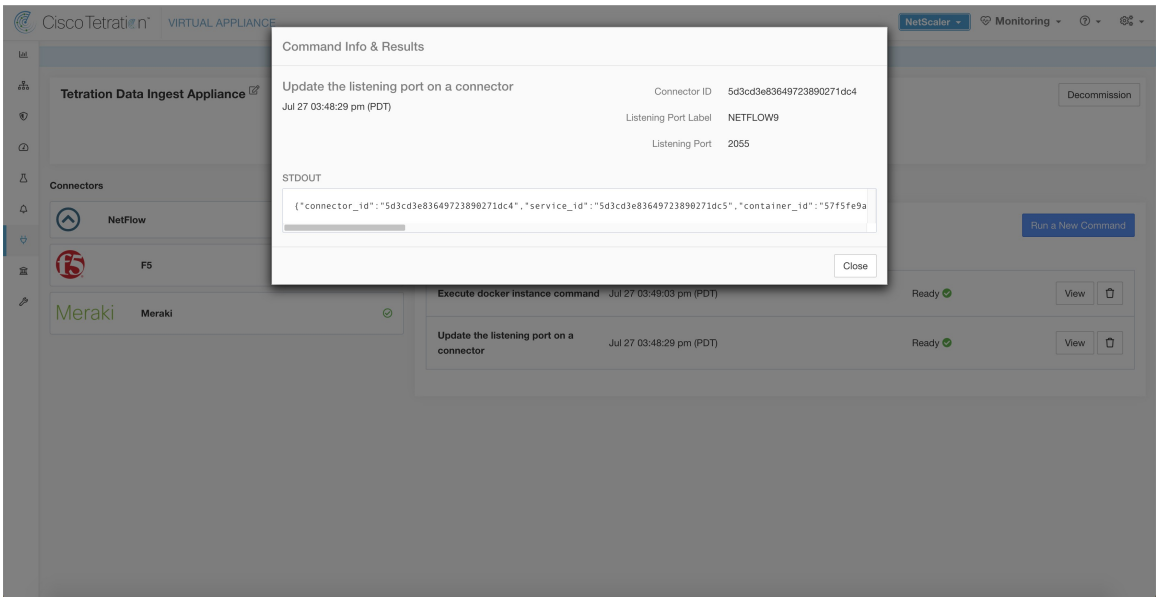
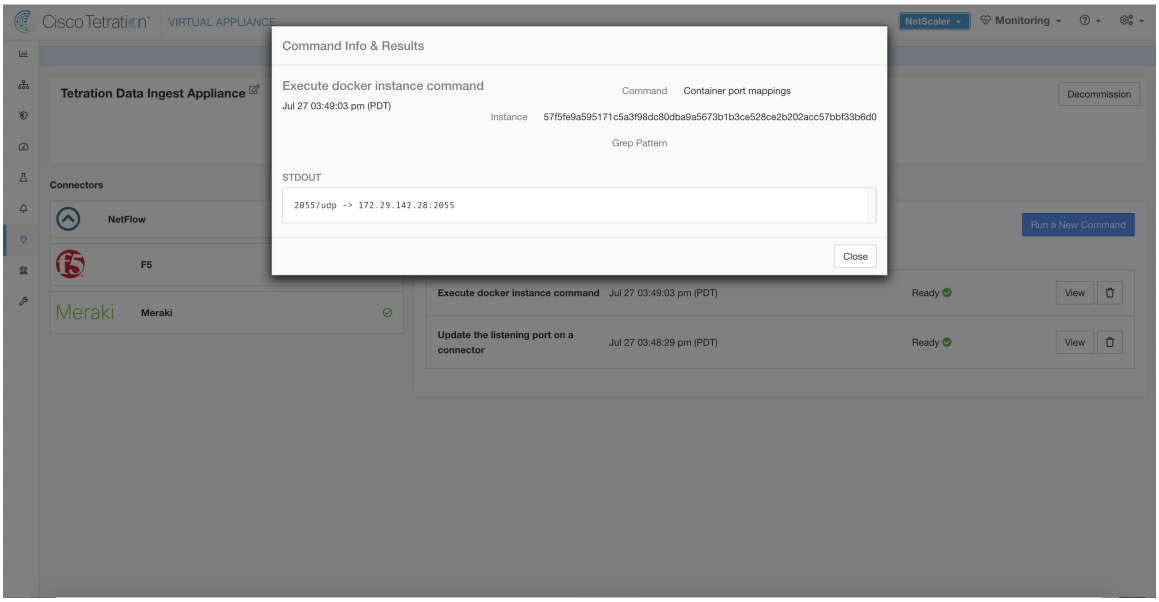


Figure 159: Récupérer les mappages de ports sur le connecteur Meraki dans l'appareil d'acquisition Cisco Secure Workload



Mettre à jour la configuration des journaux du connecteur de l'outil de notification d'alerte

Mettez à jour la configuration du journal pour le service Alert Notifier (TAN) de Cisco Secure Workloadqui héberge les connecteurs de notification d'alerte Syslog, de courriel, Slack, PagerDuty et Kinesis. Puisque le TAN héberge plusieurs connecteurs, la configuration du journal ne peut pas être mise à jour directement à partir de la page du connecteur. Cette commande autorisée permet à l'utilisateur de mettre à jour la configuration du journal.

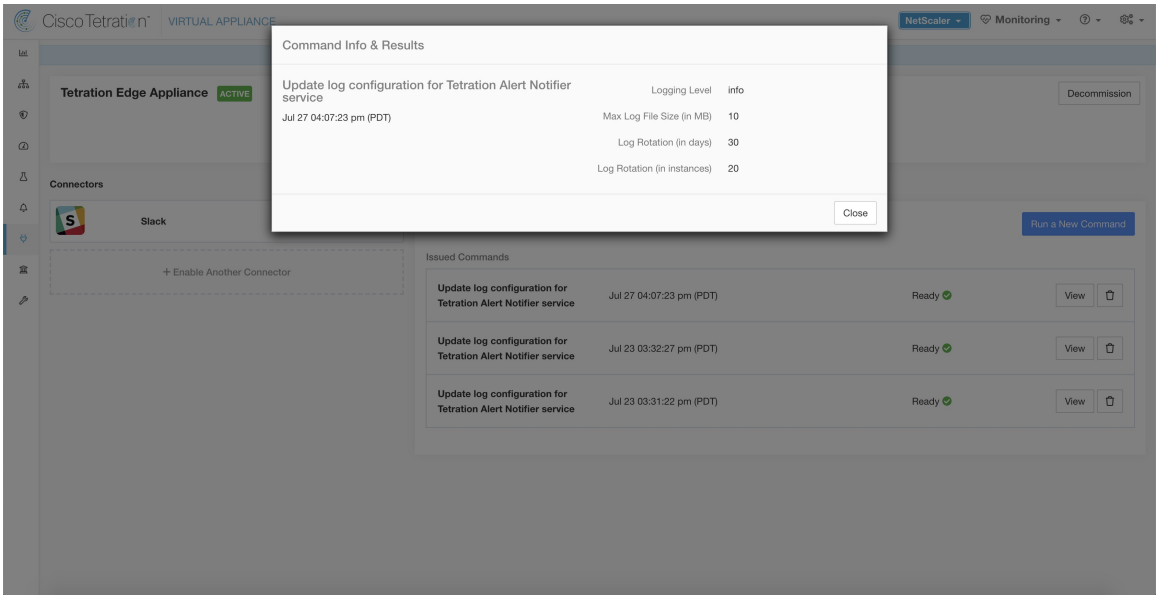
Cisco Secure Workload envoie la commande au contrôleur de service sur le service Docker TAN de l'appareil de périphérie Cisco Secure Workload. Le contrôleur applique la configuration au service et renvoie l'état de la mise à jour de la configuration.

Nom de l'argument	Type	Description
Niveau de journalisation	liste déroulante	Niveau de journalisation à utiliser par le service
	• *débogage*	Niveau de journal de débogage
	• *Information*	Niveau de journalisation informatif
	• *avertir*	Niveau du journal des avertissements
	• *erreur*	Niveau du journal des erreurs
Taille maximale du fichier journal (en Mo)	number	Taille maximale d'un fichier de journal avant le début de la rotation des journaux
Rotation des journaux (en jours)	number	Longévité maximale d'un fichier journal avant le début de la rotation des journaux
Rotation des journaux (dans les instances)	number	Nombre maximal d'instances de fichiers journaux conservées

Appliances virtuelles Cisco Secure Workload autorisées : Secure Workload Edge

Connecteurs autorisés :aucun

Figure 160: Mettre à jour la configuration des journaux sur le service Docker Alert Notifier Cisco Secure Workload dans l'appareil de périphérie Cisco Secure Workload.



Recueillir un instantané de l'appareil

Cisco Secure Workload envoie la commande à l'appareil où la commande a été exécutée. Lorsque le contrôleur de l'appareil reçoit cette commande de Cisco Secure Workload, il collecte les instantanés de l'appareil, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Fichiers inclus dans l'instantané :

- /local/tetration/appliance/appliance.conf
- /local/tetration/{logs, sqlite, user.cfg}
- /opt/tetration/tet_vm_setup/conf/tet-vm-setup.conf
- /opt/tetration/tet_vm_setup/docker/Dockerfile
- /opt/tetration/ova/version
- /usr/local/tet-controller/conf
- /usr/local/tet-controller/cert/{topic.txt, kafkaBrokerIps.txt}
- /var/run/supervisord.pid
- /etc/resolv.conf

Sorties de commande incluses dans l'instantané :

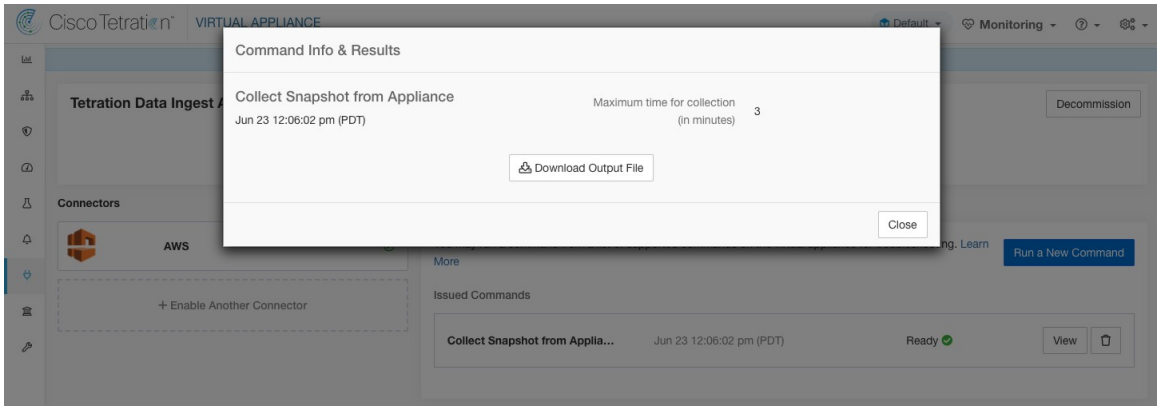
- ps aux
- iptables -L
- netstat {-nat, -rn, -suna, -stna, -tunlp}

- ss {-nat, -rn, -suna, -stna, -tunlp}
- /usr/local/tet-controller/tet-controller -version
- supervisorctl status
- rpm -qi tet-nic-driver tet-controller
- du -shc /local/tetration/logs
- ls {/usr/local/tet-controller/cert/, -l /local/tetration/sqlite/, -l /opt/tetration/tet_vm_setup/.tet_vm.done, -l/opt/tetration/tet_vm_setup/templates/}
- docker {images, ps -a}
- blkid/ifconfig/lscpu/uptime
- free -m
- df -h

Nom de l'argument	Type	Description
Durée maximale de la collecte en minutes	number	Durée maximale de la collecte avant l'envoi des résultats. Elle doit être inférieure à 20 minutes.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Figure 161: Recueillir un instantané de l'appareil Cisco Secure Workload



Recueillir l'instantané du connecteur

Cisco Secure Workload envoie la commande à l'appareil sur lequel le connecteur est déployé. Selon l'ID du connecteur, le contrôleur collecte les instantanés du connecteur, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format .tar.gz.

Fichiers inclus dans l'instantané :

- /usr/local/tet-netflow/conf

- /local/tetration/ {logs, SQLite}
- /var/run/ {supervisord.pid, tet-netflow.rid}

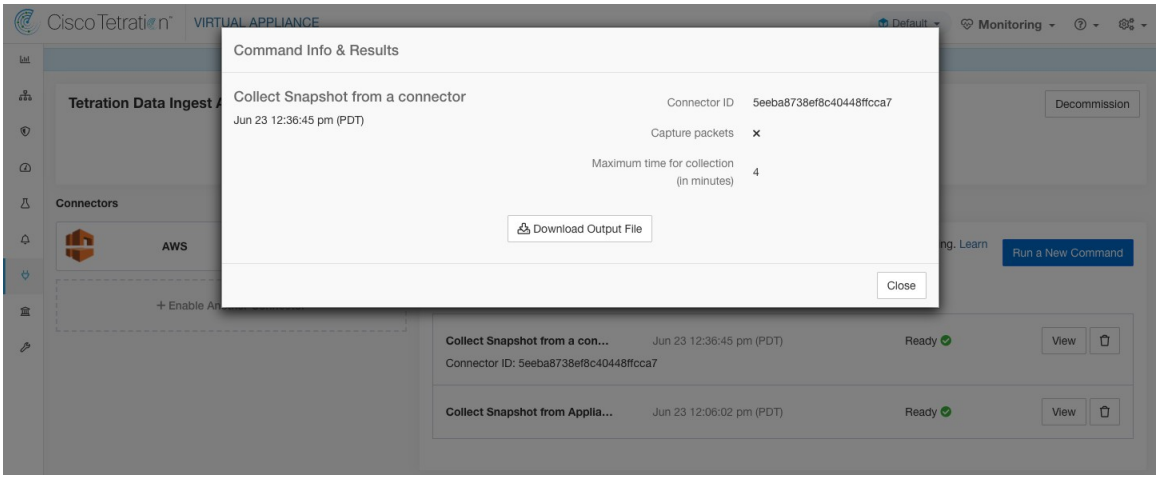
Sorties de commande incluses dans l'instantané :

- ps aux
- netstat {-nat, -rn, -suna, -stna, -tunlp}
- ss {-nat, -rn, -suna, -stna, -tunlp}

Nom de l'argument	Type	Description
ID du connecteur	chaîne	ID de connecteur du connecteur pour lequel la commande d'instantané est exécutée.
Capturer les paquets	case à cocher	Les paquets doivent-ils être capturés?
Max time for collection in minutes	number	Durée maximale de la collecte avant l'envoi des résultats. Elle doit être inférieure à 20 minutes.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Figure 162: Recueillir un instantané du connecteur Cisco Secure Workload sur l'ID de connecteur désigné



Recueillir le profil du contrôleur

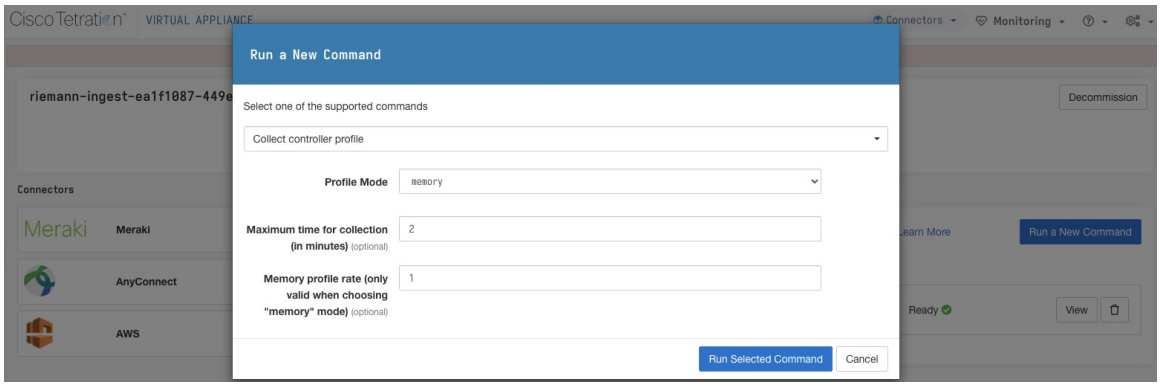
Recueillez les résultats du profilage de processus du contrôleur sur l'appareil ou les connecteurs. Cisco Secure Workload envoie la commande au connecteur où la commande a été exécutée. Le contrôleur de services redémarre le service de connecteur dans le mode de profilage spécifié. Après avoir obtenu le résultat de profilage, le contrôleur de service redémarre le service en mode normal et envoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Nom de l'argument	Type	Description
Profile Mode	liste déroulante	mode de profilage.
	• *memory*	Mode de profilage de mémoire.
	• *cpu*	mode de profilage du processeur (CPU).
	• *block*	Mode de profilage du bloc
	• *mutex*	Mode de profilage Mutex.
	• *goroutine*	Mode de profilage Goroutine.
Durée maximale de la collecte (en minutes)	number	Durée maximale de la collecte avant de renvoyer le résultat.
Débit du profil de mémoire (valide uniquement lorsque vous choisissez le mode « mémoire »)	number	Taux de profilage de mémoire. Ce champ est facultatif. S'il n'est pas fourni, la valeur par défaut dans Golan sera utilisée.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Email, Slack, PagerDuty, Kinesis, ISE, et Meraki.

Figure 163: Recueillir le profil du contrôleur de l'appareil Cisco Secure Workload



Recueillir le profil de connecteur

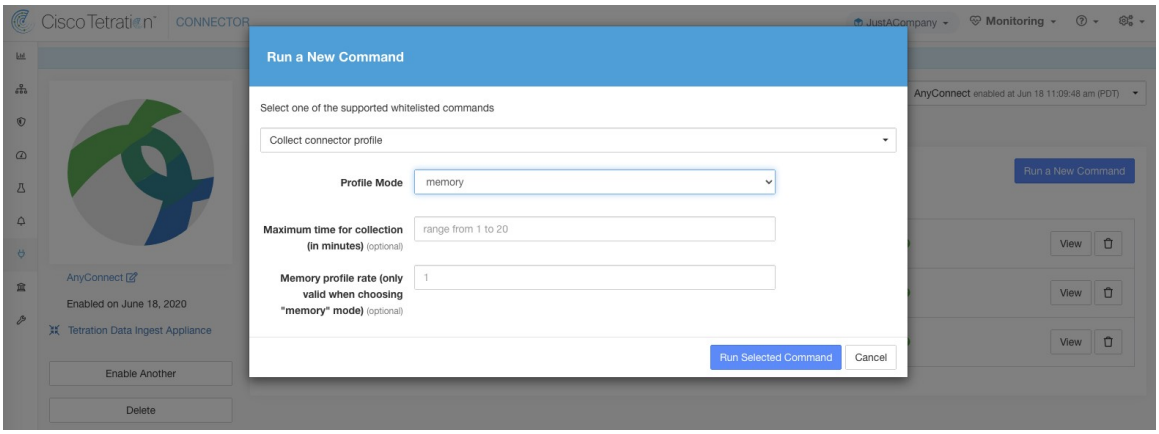
Recueillir les résultats du profilage des processus des connecteurs. Cisco Secure Workload envoie la commande au connecteur où la commande a été émise. Le contrôleur de services redémarre le service de connecteur dans le mode de profilage spécifié. Après avoir obtenu le résultat de profilage, le contrôleur de service redémarre le service en mode normal et envoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Nom de l'argument	Type	Description
Profile Mode	liste déroulante	mode de profilage.
	• *memory*	Mode de profilage de mémoire.
	• *cpu*	mode de profilage du processeur (CPU).
	• *block*	Mode de profilage du bloc
	• *mutex*	Mode de profilage Mutex.
	• *goroutine*	Mode de profilage Goroutine.
Durée maximale de la collecte (en minutes)	number	Durée maximale de la collecte avant de renvoyer le résultat.
Débit du profil de mémoire (valide uniquement lorsque vous choisissez le mode « mémoire »)	number	Taux de profilage de mémoire. Ce champ est facultatif. S'il n'est pas fourni, la valeur par défaut dans Golan sera utilisée.

Appliances virtuelles Secure Workload autorisées : Cisco Secure Workload Ingest et Cisco Secure Workload Edge

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Email, Slack, PagerDuty, Kinesis, ISE, et Meraki.

Figure 164: Recueillir le profil de connecteur du connecteur Cisco Secure Workload



Remplacer l'intervalle d'alerte du connecteur pour l'appareil

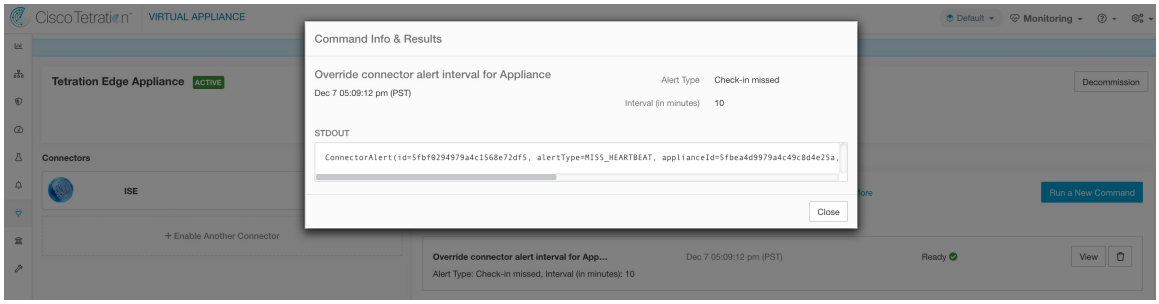
Remplacer l'intervalle d'alerte par défaut du connecteur de l'appareil. Cisco Secure Workload restreint l'envoi d'une seule alerte de connecteur par jour par défaut. Cette commande permet à l'administrateur de remplacer l'intervalle lorsqu'il estime qu'une fois par jour est trop long. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Type d'alerte	liste déroulante	Type d'alerte de connecteur à remplacer.
	• *Enregistrement manqué*	Vous avez manqué l'enregistrement de l'appareil.
	• *Utilisation du processeur*	Utilisation élevée
	• *Utilisation de la mémoire*	Utilisation élevée de la mémoire
	• *Utilisation du disque*	Utilisation élevée du disque.
Intervalle (en minutes)	number	Durée du remplacement de l'intervalle en minutes.

Appliances virtuelles Secure Workload autorisées : Cisco Secure Workload Ingest et Cisco Secure Workload Edge

Connecteurs autorisés : aucun

Figure 165: Remplacer l'intervalle d'alerte du connecteur pour l'appareil Cisco Secure Workload



Remplacer l'intervalle d'alerte du connecteur pour le connecteur

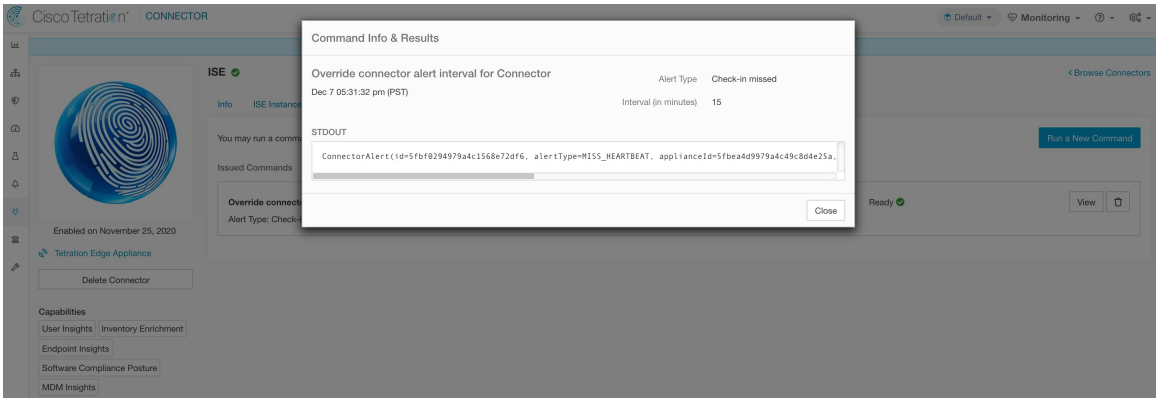
Remplacer l'intervalle d'alerte de connecteur par défaut pour le connecteur. Cisco Secure Workload restreint l'envoi à une seule alerte de connecteur par jour par défaut. Cette commande permet à l'administrateur de remplacer l'intervalle lorsqu'il estime qu'une fois par jour est trop long. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Type d'alerte	liste déroulante	Type d'alerte de connecteur à remplacer.
	• *Enregistrement manqué*	Il manque l'enregistrement du connecteur.
Intervalle (en minutes)	number	Durée du remplacement de l'intervalle en minutes.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA, Meraki, ServiceNow, WAD.

Figure 166: Remplacer l'intervalle d'alerte du connecteur pour le connecteur Cisco Secure Workload



Tableaux de bord Hawkeye

Les tableaux de bord Hawkeye fournissent des informations sur l'intégrité des connecteurs et des appliances virtuelles lorsque les connecteurs sont activés.

Tableau de bord du contrôleur d'appareil

Le tableau de bord du contrôleur d'appareil fournit des informations sur les statistiques du réseau et les mesures du système telles que le pourcentage d'utilisation du processeur, de la mémoire, du disque et le nombre de descripteurs de fichiers ouverts.

Figure 167: Tableau de bord du contrôleur d'appareil

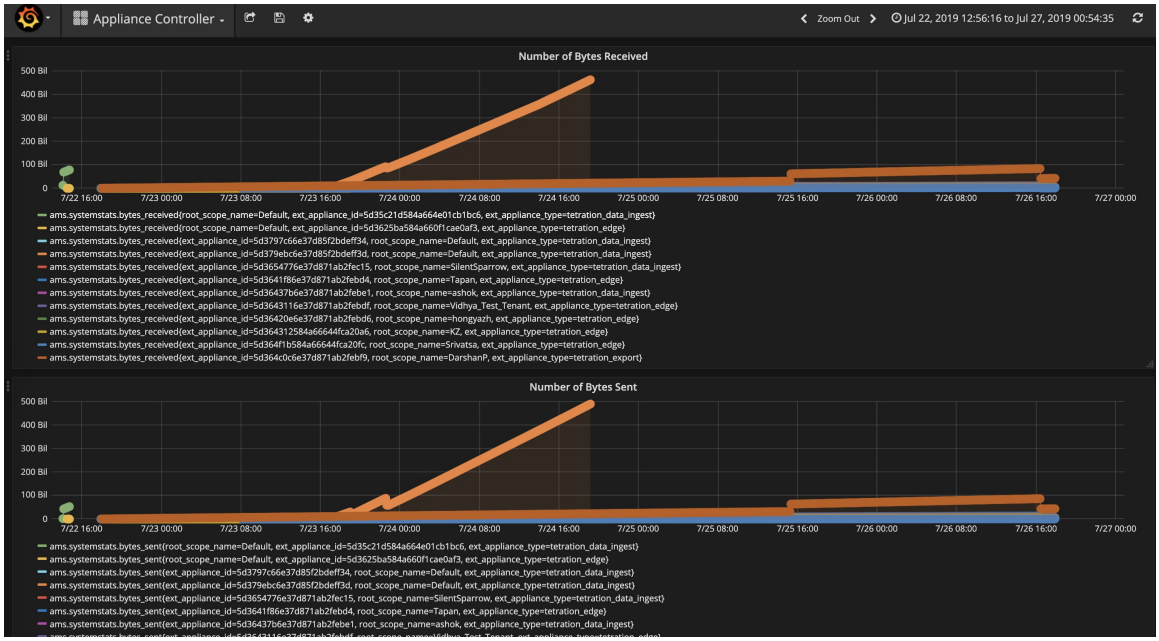


Tableau de bord du service

Le tableau de bord du service fournit des renseignements sur les mesures d'exportation, le cas échéant, y compris le nombre d'observations de flux exportées vers Cisco Secure Workload, le nombre de paquets exportés vers Cisco Secure Workload et le nombre d'octets exportés vers Cisco Secure Workload. En outre, ce tableau de bord fournit des informations sur le traitement et le décodage du protocole (par exemple, les services qui traitent NetFlow v9 et IPFIX). Des mesures telles que le nombre décodé, le nombre d'erreurs décodées, le nombre de flux, le nombre de paquets et le nombre d'octets sont disponibles dans ce tableau de bord. En outre, les mesures du système pour le conteneur Docker où le service est exécuté sont également incluses dans ce tableau de bord. Des mesures telles que le pourcentage d'utilisation du processeur, le pourcentage d'utilisation de la mémoire, le pourcentage d'utilisation du disque et le nombre de descripteurs de fichiers ouverts font partie de ce tableau de bord.

Figure 168: Tableau de bord du service

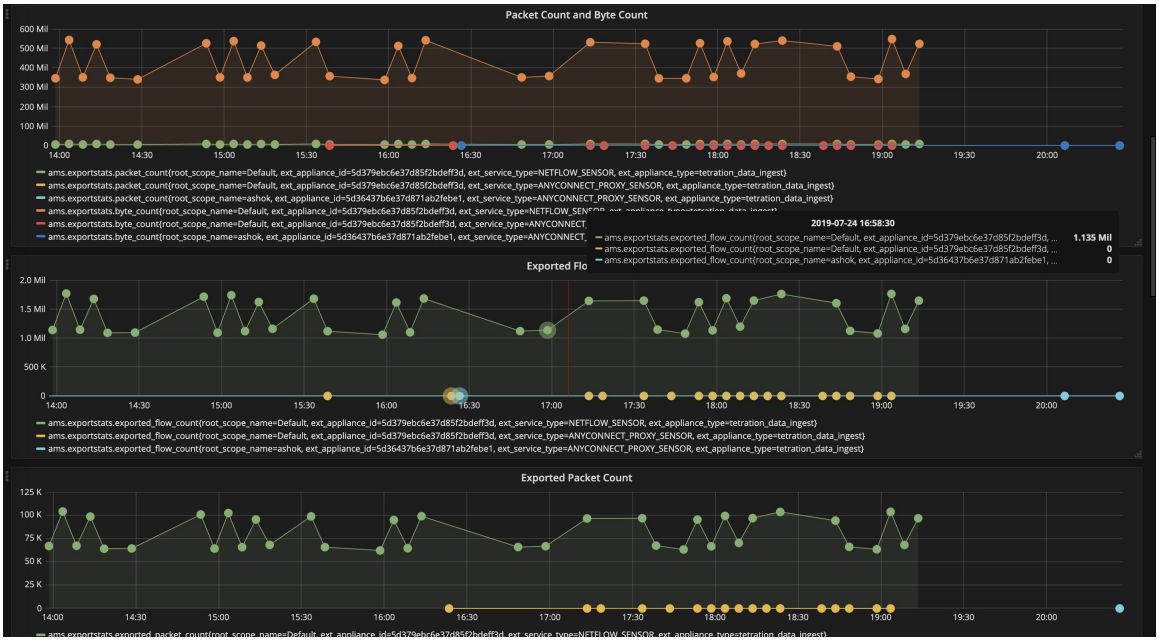


Tableau de bord du service AnyConnect

Le tableau de bord du service AnyConnect fournit des renseignements sur le service spécifique à AnyConnect. Les mesures telles que le nombre de points terminaux, le nombre d'inventaires et le nombre d'utilisateurs rapportés par le connecteur AnyConnect à Cisco Secure Workload sont disponibles dans ce tableau de bord. En outre, ce tableau de bord fournit également des renseignements sur le traitement et le décodage du protocole IPfix. Des mesures telles que le nombre décodé, le nombre d'erreurs décodées, le nombre de flux, le nombre de paquets et le nombre d'octets sont disponibles dans ce tableau de bord.

Figure 169: Tableau de bord AnyConnect

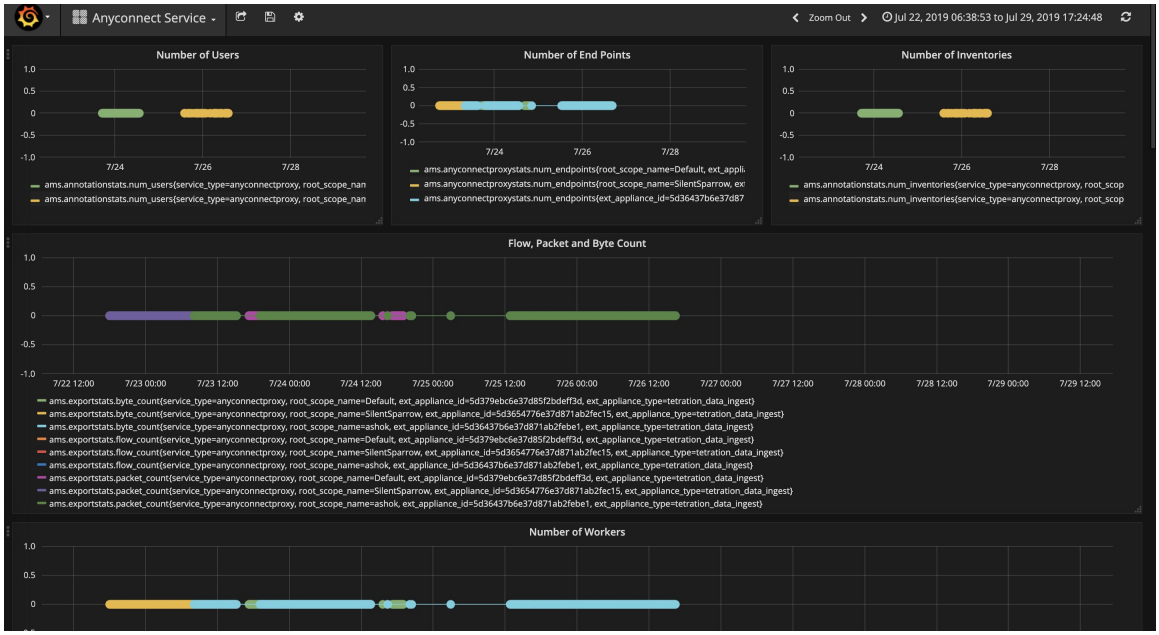
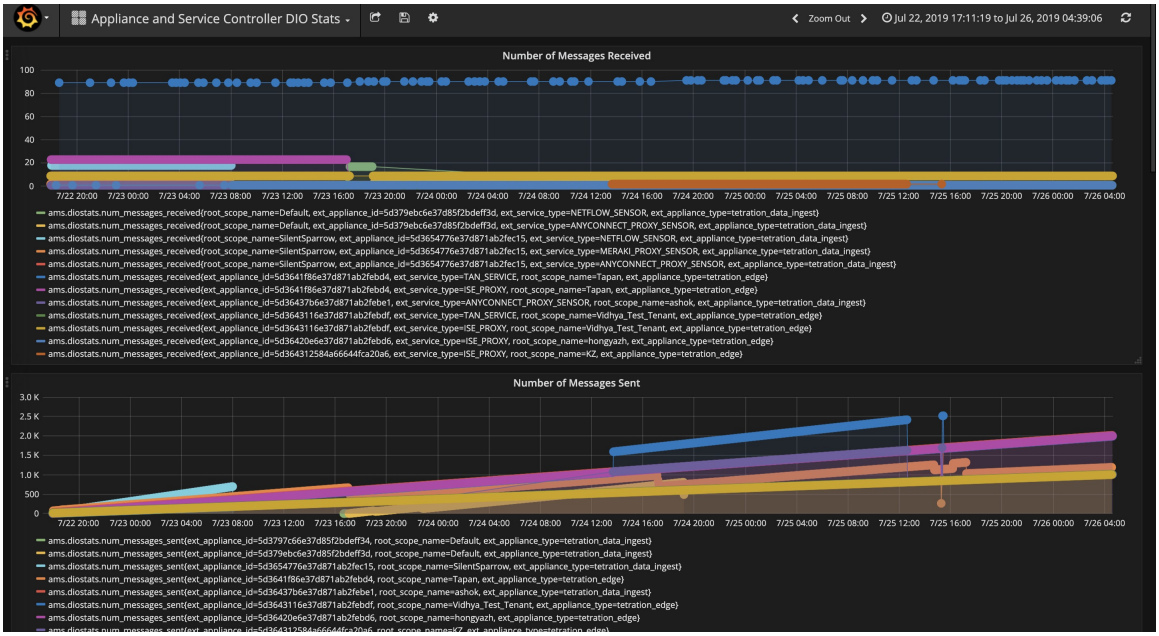


Tableau de bord de l'appareil et du service DIO

Le tableau de bord des appareils et des services DIO fournit des renseignements sur le nombre de messages échangés dans la rubrique Kafka sur laquelle communiquent le gestionnaire d'appareils et les contrôleurs des appareils et services. Des mesures telles que le nombre de messages reçus, le nombre de messages envoyés et le nombre de messages en échec sont incluses dans ce tableau de bord. En outre, le dernier décalage lu par les contrôleurs est également fourni pour comprendre si le contrôleur est en retard dans le traitement des messages de contrôle du gestionnaire.

Figure 170: Tableau de bord de l'appareil et du service DIO



Directives générales de dépannage

Une fois qu'un connecteur est affiché à l'état actif dans la page des connecteurs de Cisco Secure Workload, aucune action n'est nécessaire sur l'appareil sur lequel le connecteur est activé; l'utilisateur n'a pas besoin de s'y connecter. Si ce n'est pas le cas, les renseignements suivants vous aideront à résoudre ces problèmes.

Dans des conditions normales, sur l'appareil :

- `systemctl status tet_vm_setup.service` signale un service *inactif* avec l'état de sortie *SUCCESS*.
- `systemctl status tet-nic-driver` signale un service *actif* .
- `supervisorctl status tet-controller` signale un service *RUNNING (EN COURS D'EXÉCUTION)* . Cela indique que le contrôleur de l'appareil est opérationnel.
- `docker network ls` signale trois réseaux : `pont`, `hôte` et `aucun`.
- `docker ps` signale les conteneurs en cours d'exécution sur l'appareil. En règle générale, lorsqu'un connecteur est activé avec succès sur un appareil, un conteneur Docker est instancié sur l'appareil. Pour les connecteurs Syslog, Courriel, Slack, PagerDuty et Kinesis, un service de notification d'alertes Cisco Secure Workload est instancié en tant que conteneur Docker sur l'appareil de périphérie Cisco Secure Workload.
- `docker logs <cid>` pour chaque conteneur doit signaler que tet-netflowensor est entré à l'état RUNNING.
- `docker exec <cid> ifconfig` ne signale qu'une seule interface, en plus de la boucle avec retour;
- `docker exec <cid> netstat -rn` signale la passerelle par défaut.
- `cat /local/tetration/appliance/appliance.conf` sur l'appareil pour voir la liste des services Docker en cours d'exécution sur celui-ci. Il comprend des détails sur l'ID de service, l'ID du connecteur, le conteneur, l'ID d'image et les mappages de port (le cas échéant). Sur un appareil d'acquisition Cisco

Secure Workload, trois services au maximum doivent être exécutés sur l'appareil. Les mappages de ports et les volumes Docker montés sur les conteneurs sont disponibles dans ce fichier.

Figure 171: Service et état de déploiement d'appareils Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# systemctl status tet_vm_setup.service
● tet_vm_setup.service - Tetration Appliance Setup
   Loaded: loaded (/etc/systemd/system/tet_vm_setup.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Sat 2019-07-27 23:51:29 UTC; 21h ago
 Main PID: 1249 (code=exited, status=0/SUCCESS)

Jul 27 23:51:12 localhost.localdomain python[1249]: mount: /dev/sr0 is write-protected, mounting read-only
Jul 27 23:51:29 esx-2106-ingest python[1249]: Docker version 18.09.8, build 0dd43dd87f
Jul 27 23:51:29 esx-2106-ingest python[1249]: REPOSITORY          TAG                 IMAGE ID            CREATE... SIZE
Jul 27 23:51:29 esx-2106-ingest python[1249]: userPrivateKey.key
Jul 27 23:51:29 esx-2106-ingest python[1249]: intermediateCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaBrokerIps.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: userCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: topic.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: Created symlink from /etc/systemd/system/multi-user.target.wants/s...vice.
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 172: État du service de pilote réseau Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# systemctl status tet-nic-driver.service
● tet-nic-driver.service - NIC network driver plugin for Docker
   Loaded: loaded (/etc/systemd/system/tet-nic-driver.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2019-07-27 23:51:12 UTC; 21h ago
 Main PID: 733 (nic)
   Memory: 4.4M
   CGroup: /system.slice/tet-nic-driver.service
           └─733 /usr/local/tet/nic-driver/nic -log-level debug

Jul 27 23:51:12 localhost.localdomain systemd[1]: Started NIC network driver plugin for Docker.
Jul 27 23:51:12 localhost.localdomain systemd[1]: Starting NIC network driver plugin for Docker...
Jul 27 23:51:12 localhost.localdomain nic[733]: time="2019-07-27T23:51:12Z" level=info msg="NIC network driver started"
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 173: État du contrôleur de l'appareil

```
[root@esx-2106-ingest tetter]# supervisorctl status tet-controller
tet-controller                   RUNNING   pid 1971, uptime 21:43:29
[root@esx-2106-ingest tetter]#
```

Si l'une des situations précédentes n'est pas vérifiée, vérifiez les journaux du script de déploiement dans /local/tetration/logs pour connaître la raison de l'échec du déploiement de l'appareil et/ou du connecteur.

Vous pouvez résoudre tout autre problème d'enregistrement ou de connectivité du connecteur comme suit.

`docker exec <cid> ps -ef` signale les instances tet-netflowsensor-engine, `/usr/local/tet/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf`, ainsi que l'instance de gestionnaire de processus `/usr/bin/supervisord -c /usr/local/tet-netflow/ conf/supervisord.conf -n`.

Figure 174: Exécution des processus sur le connecteur ASA de Cisco Secure Firewall dans le dispositif d'acquisition Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# docker ps
CONTAINER ID        IMAGE                                                                                COMMAND
     CREATED             STATUS              PORTS                                NAMES
c82decfaa877        asa_sensor-3.4.2.52465.appliance.demo.mrpm.build-asa:5d3ce5e43649723890271dd3   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours         172.29.142.27:4729->4729/udp   asa-5d3ce5e43649723890271dd3
eddd5cd59839        aws_sensor-3.4.2.52465.appliance.demo.mrpm.build-aws:5d3ce3b73649723890271dce   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours                                      aws-5d3ce3b73649723890271dce
[root@esx-2106-ingest tetter]# docker exec c8 ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 00:01 ?        00:00:15 /usr/bin/python /usr/bin/supervisord -c /usr/local/tet-netflow/conf/supe
rvisord.conf -n
root         8     1  0 00:01 ?        00:02:24 /usr/local/tet-netflow/tet-netflowsensor-engine -ctrl-config /usr/local/
tet-netflow/conf/tet-controller.conf -upgrade-script /usr/local/tet-netflow/scripts/check_config_update.sh -service /usr
/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf
root     27002     8  0 21:31 ?        00:00:00 /usr/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/
conf/tet-netflow.conf
root     27024     0  0 21:32 ?        00:00:00 ps -ef
[root@esx-2106-ingest tetter]#
```

Journaliser les fichiers

Les commandes suivantes peuvent être utilisées pour afficher les journaux de divers services sur l'appareil.

- **/local/tetration/logs/tet-controller.log** affiche les journaux du contrôleur d'appareil.
- **docker exec <cid> cat /local/tetration/logs/tet-controller.log** affiche les journaux du contrôleur de service sur le connecteur.
- **exécutable Docker** <cid> cat /local/tetration/logs/tet-netflow.log affiche les journaux du service de connecteur.
- **docker exec <cid> cat /local/tetration/logs/tet-ldap-loader.log** affiche les journaux de création d'instantané LDAP (si la configuration LDAP est applicable au connecteur).
- **docker exec <cid> cat /local/tetration/logs/check_conf_update.log** affiche les journaux d'interrogation de la mise à jour de la configuration (pour les connecteurs sur l'appareil d'acquisition).

Note Il existe un ensemble autorisé de commandes sur Cisco Secure Workload qui peuvent extraire ces journaux de l'appareil et/ou des connecteurs directement. Pour en savoir plus, consultez Ensemble de commandes autorisé.

Mode de débogage

Le niveau de journalisation par défaut pour l'appareil/le contrôleur de service et le service de connecteur est défini au niveau *info*. Pour résoudre les problèmes, il se peut que nous devions définir l'agent en mode *débogage*. Pour ce faire, mettez à jour la configuration du journal sur l'appareil/le connecteur sur Cisco Secure Workload directement pour l'appareil ou le connecteur souhaité. Les niveaux de journalisation du contrôleur et des services sont mis à jour si la configuration est mise à jour sur le connecteur. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Cisco Secure Firewall Management Center

Combine the power of Cisco Secure Workload with the power of Cisco's Secure Firewall (formerly known as Cisco Firepower) for a security solution that makes use of:

- Segmentation

  Firewall-based segmentation is suitable for workloads where software agents are not installed. However, you can also use this method for agent-based workloads. You can easily and broadly apply different sets of policies for traffic entering your network, for traffic exiting your network, and for traffic between workloads within your network.

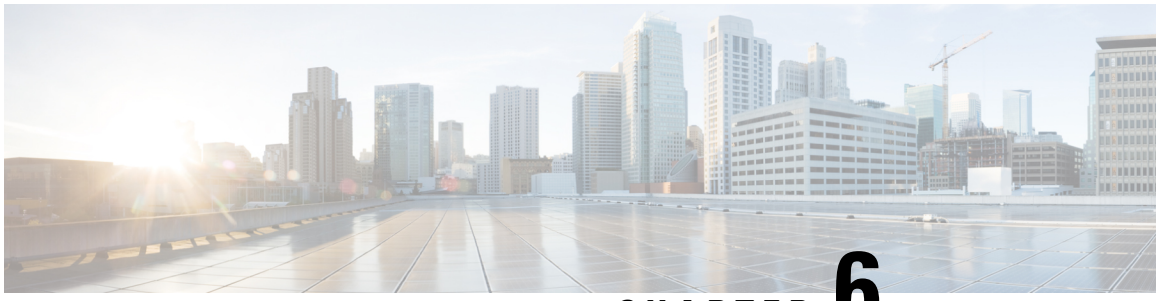
- Virtual Patching

  Virtual patching adds Intrusion Prevention System (IPS) protection to workloads where software agents are installed. Use this integration to avoid malicious traffic entering the application. With the Virtual Patching Config, Secure Workload publishes the CVEs to the FMC to consider while creating the IPS policies.

With this integration, Secure Workload automatically enforces and manages segmentation policies on the Secure Firewall Threat Defense (formerly known as Firepower Threat Defense) firewalls managed by the Secure Firewall Management Center instance. Policies are updated dynamically, and the set of workloads to which policies apply is refreshed continually as the application environment changes.

Network inventory is dynamically updated by the Secure Workload inventory filters on which your segmentation policies are based; when workloads are added, changed, or removed from your network, Secure Workload automatically updates the Dynamic Objects in Secure Firewall Management Center on which the corresponding access control rules are based. All enforced policy changes are automatically deployed to managed Secure Firewall Threat Defense (formerly known as Firepower Threat Defense or FTD) devices; you never need to redeploy changes in Secure Firewall Management Center.

For complete information about this integration, including more details about how it works, supported platforms, limitations, setup instructions for both products, and troubleshooting information, see the Cisco Secure Workload and Cisco Secure Firewall Management Center Integration Guide.



CHAPTER 6

Inventory

Inventory is the IP addresses of all the workloads on your network, annotated with labels and other data that describes them. Your inventory includes workloads running on bare metal or virtual machines, in containers, and in the cloud. If applicable, it may also include workloads running on partner networks.

Collecting inventory data is an iterative process. Data from different sources for a single IP address can be merged, and new and changed IP addresses can be updated. Over time, management of your inventory should become increasingly dynamic.

You will work with and group your inventory using searches, filters, and scopes, based on the labels and annotations that are associated with each inventory item. Policies are applied to groups of workloads that are defined by the filters and scopes you define for your inventory.

Options for working with inventory vary depending on your role but may include **Search**, **Filters**, and **Upload**.

Étiquettes de charge de travail

Les étiquettes (parfois appelées balises, annotations, attributs, métadonnées ou contexte, bien que ces termes ne soient pas toujours complètement synonymes) sont la clé de la puissance de Cisco Secure Workload.

Des étiquettes lisibles par un humain décrivent vos charges de travail selon leur fonction, leur emplacement et d'autres critères.

Cisco Secure Workload prend en charge les méthodes suivantes pour l'ajout d'étiquettes d'utilisateur :

- Découverte par les agents Cisco Secure Workload exécutés sur les éléments de l'inventaire
- Importation manuelle à partir de fichiers de valeurs séparées par des virgules (CSV)

- Affectation manuelle au moyen de l'interface utilisateur
- Importation automatisée à l'aide des Connecteurs pour points terminaux
- Importation automatisée à l'aide des connecteurs pour l'enrichissement de l'inventaire
- Importation automatisée des étiquettes générées et personnalisées par l'orchestrateur (voir Orchestrateurs externes dans Cisco Secure Workload)
- Importation automatisée à partir de connecteurs infonuagiques (voir connecteurs infonuagiques)
- Vous pouvez spécifier des étiquettes d'inventaire lors de la création du script d'installation. Tous les agents installés à l'aide du script reçoivent automatiquement ces étiquettes. Seuls les déploiements de charges de travail Linux et Windows prennent en charge cette fonctionnalité.

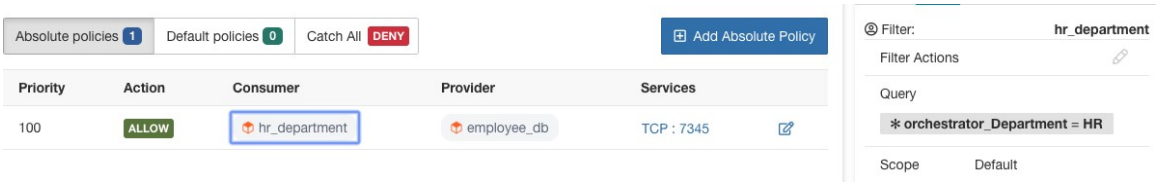
Importance des étiquettes

Les étiquettes vous permettent de définir une politique logique. Par exemple :

autoriser le trafic du consommateur hr_department au fournisseur employee_db

Plutôt que de préciser les membres des groupes de charges de travail de consommateurs et de fournisseurs, nous pouvons définir la politique logique à l'aide des étiquettes, comme le montre la figure suivante. Notez que cela permet de modifier dynamiquement les membres des groupes de consommateurs et de fournisseurs sans qu'il soit nécessaire de modifier la politique logique. Au fur et à mesure que des charges de travail sont ajoutées et retirées, Cisco Secure Workload est averti par les services que vous avez configurés, tels que les orchestrateurs externes et les connecteurs infonuagiques. Cela permet à Cisco Secure Workload d'évaluer l'appartenance au groupe de consommateurs *hr_department* et au groupe de fournisseurs *employee_db*.

Figure 175: Exemple de politique avec des étiquettes



Héritage d'étiquette basé sur le sous-réseau

L'héritage d'étiquette basé sur le sous-réseau est pris en charge. Les adresses IP et les sous-réseaux plus restreints héritent des étiquettes des sous-réseaux plus importants dont ils relèvent lorsque l'une des conditions suivantes est satisfaite :

- L'étiquette ne figure pas dans la liste des étiquettes pour le sous-réseau ou l'adresse de niveau inférieur.
- La valeur d'étiquette pour le sous-réseau/adresse de niveau inférieur est vide.

Considérez l'exemple suivant :

IP	Nom	Objectif	Environnement	Esprit-animal
10.0.0.1	Serveur 1	Trafic Web	production	
10.0.0.2				grenouille

IP	Nom	Objectif	Environnement	Esprit-animal
10.0.0.3				aigle
10.0.0.0/24	vlan Web		intégration	
10.0.0.0/16		Trafic Web		blaireau
10.0.0.0/8			test	ours

Les étiquettes pour l'adresse IP *10.0.0.3* sont *{« nom » : « Vlan Web », « objectif » : « trafic Web », « environnement » : « intégration », « esprit-animal »: « aigle »}*.

Préfixes d'étiquettes

Les étiquettes sont automatiquement affichées, avec un préfixe qui identifie la source des renseignements.

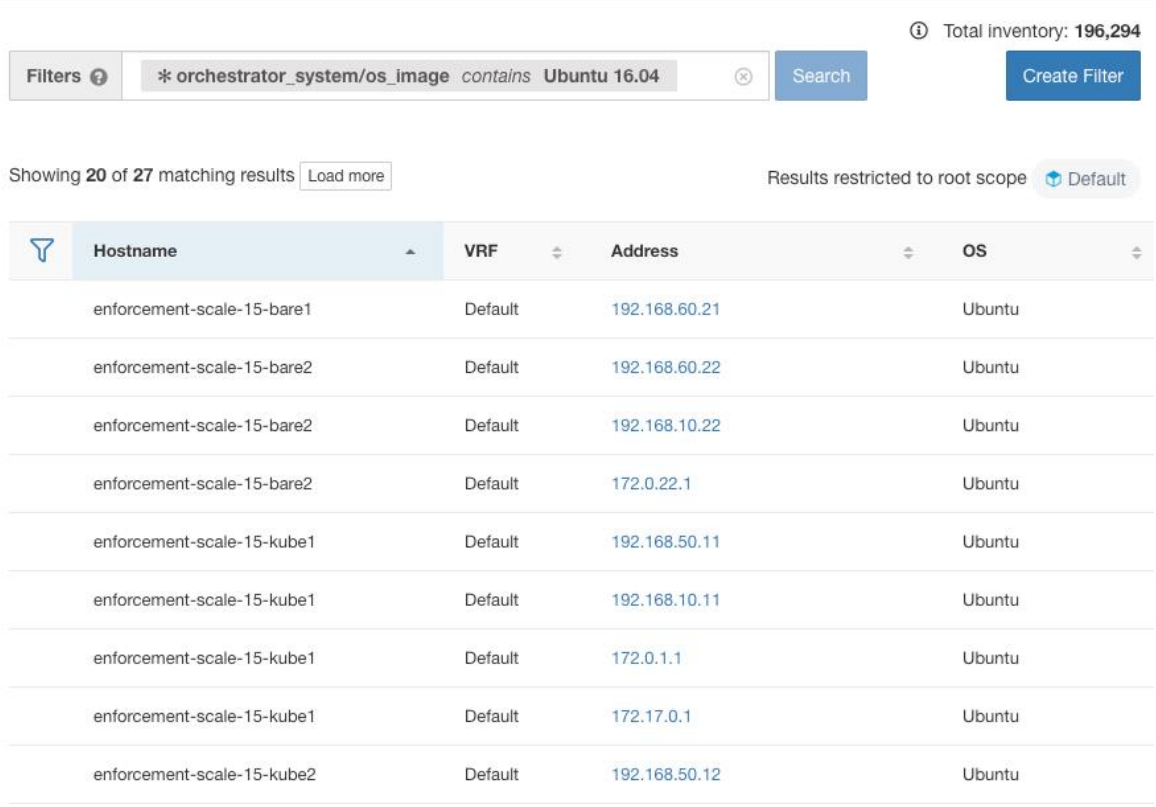
Toutes les étiquettes d'utilisateur sont précédées de * dans l'interface utilisateur (*user_* dans OpenAPI). En outre, les étiquettes importées automatiquement à partir d'orchestrateurs externes ou de connecteurs infonuagiques portent le préfixe orchestrator_. Pour les étiquettes importées à partir de connecteurs de point terminal, consultez les détails dans la section Connecteurs pour points terminaux, mais peut inclure des étiquettes précédées de *ldap_*.

Par exemple, une étiquette avec une clé de *department* (service) importée à partir de fichiers CSV téléversés par l'utilisateur apparaît dans l'interface utilisateur en tant que * *department* et dans OpenAPI en tant que *user_department*. Une étiquette avec une clé *location* (emplacement) importée d'un orchestrateur externe apparaît dans l'interface utilisateur en tant que * *orchestrator_location* et dans OpenAPI en tant que *user_orchestrator_location*.

La figure suivante montre un exemple de recherche dans l'inventaire utilisant l'étiquette générée par l'orchestrateur en utilisant le préfixe :

orchestrator_system/os_image:

Figure 176: Exemple de recherche d'inventaire avec des étiquettes générées par l'orchestrateur



Étiquettes générées par les connecteurs infonuagiques

Ces étiquettes s'appliquent aux données AWS et Azure. La source de ces étiquettes provient des charges de travail et des interfaces réseau d'un réseau virtuel AWS ou Azure. Les balises de la source sont fusionnées et affichées dans Cisco Secure Workload. Par exemple, si la balise de charge de travail est

```
env: prod
```

et la balise de l'interface réseau est

```
env: prod
```

, la valeur de l'étiquette dans Cisco Secure Workload est

```
prod,test
```

, qui s'affiche dans la colonne **orchestrator_env** sur la page du connecteur respective.

Pour connaître les étiquettes propres à AKS, EKS et GKE, consultez également les étiquettes relatives aux grappes Kubernetes.

Table 20: Étiquettes dans l'inventaire effectué à l'aide d'un connecteur infonuagique

Clé	Valeur
orchestrator_system/orch_type	AWS ou Azure

Clé	Valeur
orchestrator_system/cluster_name	*<Cluster_name est le nom donné par l'utilisateur pour la configuration de ce connecteur>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/cluster_id	*<ID du réseau virtuel>*

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à chaque nœud :

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*<Numéro d'instance attribué par la plateforme>*
orchestrator_system/machine_name	<PublicDNS(Nom de domaine complet) attribué à ce nœud par AWS>-ou-<Nom d'instance dans Azure>
orchestrator_system/segmentation_enabled	*<Indicateur permettant de déterminer si la segmentation est activée sur l'inventaire>*
orchestrator_system/virtual_network_id	*<ID du réseau virtuel auquel l'inventaire appartient>*
orchestrator_system/virtual_network_name	*<Nom du réseau virtuel auquel appartient l'inventaire>*
orchestrator_system/interface_id	<Identifiant de l'interface réseau élastique attachée à cet inventaire>
orchestrator_system/region	<Région à laquelle appartient l'inventaire>
orchestrator_system/resource_group	(Cette balise s'applique uniquement à l'inventaire Azure)
orchestrator_'<Tag Key>'	<Valeur de l'étiquette>Paire valeur-clé pour un nombre quelconque de balises personnalisées affectées à l'inventaire dans le portail infonuagique.

Étiquettes liées aux grappes Kubernetes

Les informations suivantes s'appliquent à Kubernetes standard, OpenShift et à Kubernetes exécuté sur les plateformes infonuagique prises en charge (EKS, AKS et GKE).

Pour chaque type d'objet, Cisco Secure Workload importe l'inventaire en direct à partir d'une grappe Kubernetes, y compris les étiquettes associées à l'objet. Les clés et les valeurs d'étiquettes sont importées telles quelles.

En plus d'importer les étiquettes définies pour les objets Kubernetes, Cisco Secure Workload génère également des étiquettes qui facilitent l'utilisation de ces objets dans les filtres d'inventaire. Ces étiquettes supplémentaires sont particulièrement utiles pour définir les portées et les politiques.

Générer des étiquettes pour toutes les ressources

Cisco Secure Workload ajoute les étiquettes suivantes à tous les nœuds, pods et services récupérés du serveur d'API Kubernetes/OpenShift/EKS/AKS/GKE.

Clé	Valeur
orchestrator_system/orch_type	kubernetes
orchestrator_system/cluster_id	*<L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload>*
orchestrator_system/cluster_name	*<Nom de la grappe Kubernetes>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/namespace	*<L'espace de noms Kubernetes/OpenShift/EKS/AKS/GKE de cet élément>*

Étiquettes propres au nœud

Les étiquettes suivantes sont générées pour les nœuds uniquement.

Clé	Valeur
orchestrator_system/workload_type	Machine
orchestrator_system/machine_id	*<UUID attribué par Kubernetes/OpenShift>*
orchestrator_system/machine_name	*<Nom donné à ce nœud>*
orchestrator_system/kubelet_version	*<Version du kubelet fonctionnant sur ce nœud>*
orchestrator_system/container_runtime_version	*<La version du conteneur en cours d'exécution sur ce nœud>*

Étiquettes spécifiques aux pods

Les étiquettes suivantes sont générées pour les pods uniquement.

Clé	Valeur
orchestrator_system/workload_type	pod
orchestrator_system/pod_id	*<UUID attribué par Kubernetes/OpenShift>*
orchestrator_system/pod_name	*<Nom donné à ce pod>*
orchestrator_system/hostnetwork	*<vrai|faux>indiquant si le pod est en cours d'exécution dans le réseau hôte*
orchestrator_system/machine_name	*<Nom du nœud sur lequel le pod est exécuté>*
orchestrator_system/service_endpoint	*[Liste des noms de services fournis par ce pod]*

Étiquettes propres au service

Les étiquettes suivantes sont générées pour les services uniquement.

Clé	Valeur
orchestrator_system/workload_type	service
orchestrator_system/service_name	*<Nom donné à ce service>*

- (Pour Kubernetes géré infonuagique uniquement) Les services de type ServiceType : Équilibreur de charge sont pris en charge uniquement pour la collecte de métadonnées, et non pour la collecte de données de flux ou pour l'application de politiques.

Tip Le filtrage des éléments à l'aide de **orchestrator_system/service_name** n'est pas la même chose que l'utilisation de **orchestrator_system/service_endpoint**.

Par exemple, l'utilisation du filtre **orchestrator_system/service_name=web** sélectionne tous les *services* avec le nom **web** tandis que **orchestrator_system/service_endpoint=web** sélectionne tous les *pods* qui fournissent un service avec le nom **web**.

Exemple d'étiquettes pour les grappes Kubernetes

L'exemple suivant montre une représentation YAML partielle d'un nœud Kubernetes et les étiquettes correspondantes importées par Cisco Secure Workload.

```
- apiVersion: v1
kind: Node
metadata:
  annotations:
    node.alpha.kubernetes.io/ttl: "0"
    volumes.kubernetes.io/controller-managed-attach-detach: "true"
  labels:
    beta.kubernetes.io/arch: amd64
    beta.kubernetes.io/os: linux
    kubernetes.io/hostname: k8s-controller
```

Table 21: Étiquettes clés importées de Kubernetes

Clés d'étiquette importées
orchestrator_beta.kubernetes.io/arch
orchestrator_beta.kubernetes.io/os
orchestrator_kubernetes.io/hostname
orchestrator_annotation/node.alpha.kubernetes.io/ttl
orchestrator_annotation/volumes.kubernetes.io/controller-managed-attach-detach
orchestrator_system/orch_type
orchestrator_system/cluster_id

Clés d'étiquette importées
orchestrator_system/cluster_name
orchestrator_system/namespace
orchestrator_system/workload_type
orchestrator_system/machine_id
orchestrator_system/machine_name
orchestrator_system/kubelet_version
orchestrator_system/container_runtime_version

Importation d'étiquettes personnalisées

Vous pouvez téléverser ou attribuer manuellement des étiquettes personnalisées pour associer des données définies par l'utilisateur à des hôtes spécifiques. Ces données définies par l'utilisateur sont utilisées pour annoter les flux et l'inventaire associés.

Il y a des limites sur le nombre d'adresses IPv4/IPv6 et de sous-réseaux qui peuvent être étiquetés dans toutes les portées racine, quelle que soit la source de l'étiquette (saisie manuellement ou téléversée, intégrée à l'aide de connecteurs ou d'orchestrateurs externes, etc.). Pour en savoir plus, consultez Limites des étiquettes.

Lignes directrices pour le chargement de fichiers d'étiquettes

Procedure

Étape 1 Pour afficher un exemple de fichier, dans le volet gauche, sélectionnez **Organize(Organiser)** > **Label Management (Gestion des étiquettes)** > **User Defined Label Upload**(Chargement d'étiquettes définies par l'utilisateur) , puis cliquez sur **Download a Sample** (Télécharger un exemple).

Étape 2 Les fichiers CSV utilisés pour charger les étiquettes utilisateur doivent inclure une clé d'étiquette (adresse IP).

Étape 3 Pour utiliser des caractères non latins dans les étiquettes, le fichier CSV doit être au format UTF-8.

Étape 4 Assurez-vous que les fichiers CSV respectent les directives décrites dans la section Schéma de clé d'étiquette.

Étape 5 Tous les fichiers téléversés doivent suivre le même schéma.

Schéma de clé d'étiquette

Lignes directrices régissant les noms de colonne

- Il doit y avoir une colonne avec un en-tête « IP » dans le schéma de clé d'étiquette. En outre, il doit y avoir au moins une autre colonne avec des attributs pour l'adresse IP.

- La colonne « VRF » revêt une signification particulière dans le schéma d'étiquette. Si elle figure, elle doit correspondre à la portée racine dans laquelle vous téléversez les étiquettes. Elle est obligatoire lors du chargement du fichier CSV à l'aide API indépendantes de la portée.
- Les noms de colonne ne peuvent contenir que les caractères suivants : des lettres, des chiffres, des espaces, des tirets, des traits de soulignement et des barres obliques.
- Les noms de colonne ne peuvent pas dépasser 200 caractères.
- Les noms de colonnes ne peuvent pas comporter le préfixe « orchestrator_ », « TA_ », « ISE_ », « SNOW_ » ou « LDAP_ », car ils peuvent entrer en conflit avec les étiquettes des applications internes.
- Le fichier CSV ne doit pas contenir de noms de colonnes en double.

Directives régissant les valeurs de colonne

- Le nombre de caractères du nom est limité à 255. Toutefois, ils doivent être aussi courts que possible tout en restant clairs, caractéristiques et significatifs pour les utilisateurs.
- Les clés et les valeurs ne sont pas sensibles à la casse. Cependant, une cohérence est recommandée.
- Les adresses figurant dans la colonne « IP » doivent être conformes au format suivant :
  - Les adresses IPv4 peuvent être au format « x.x.x.x » et « x.x.x.x/32 ».
  - Les sous-réseaux IPv4 doivent être du format « x.x.x.x/<netmask>, où netmask est un entier compris entre 0 et 31.
  - Les adresses IPv6 au format long (« x:x:x:x:x:x:x:x » ou « x:x:x:x:x:x:x:x/128 ») et au format canonique (« x:x::x » ou « x:x::x/128 ») sont pris en charge.
  - Les sous-réseaux IPv6 au format long (« x:x:x:x:x:x:x:x/<netmask> ») et le format canonique (« x:x::x/<netmask> » sont pris en charge. Le masque réseau doit être un entier compris entre 0 et 127.

L'ordre des colonnes n'a pas d'importance. Les 32 premières colonnes définies par l'utilisateur seront automatiquement activées en vue de l'étiquetage. Si plus de 32 colonnes sont téléversées, vous pouvez en activer jusqu'à 32 en utilisant les cases à cocher à droite de la page.

Charger des étiquettes personnalisées

Les étapes suivantes expliquent comment les utilisateurs ayant un rôle d' **administrateur de site**, **d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent charger des étiquettes.

Before you begin

Pour charger les étiquettes personnalisées, créez un fichier CSV selon les directives de la section sur le chargement des fichiers d'étiquettes.

Procedure

Étape 1 Dans le volet gauche, sélectionnez **Organize (Organiser)** > **User Defined Label Upload(Chargement d'étiquettes définies par l'utilisateur)** > **CSV Upload (Chargement CSV)**, puis sous **Upload New Labels**(Télécharger de nouvelles étiquettes), cliquez sur **Select File** (Sélectionner un fichier).

Étape 2 Dans le volet gauche, sélectionnez **Organize (Organiser)** > **Label Management (Gestion des étiquettes)**, puis sous **Upload New Labels** (Télécharger de nouvelles étiquettes), cliquez sur **Select File** (Sélectionner un fichier).

Étape 3 Sélectionnez l'opération Ajouter, Fusionner ou Supprimer.

- **Add (Ajouter) :** Ajoute des étiquettes aux adresses ou aux sous-réseaux nouveaux et existants. Résout les conflits en sélectionnant les nouvelles étiquettes plutôt que les existantes. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 »}* et que le fichier CSV contient *{« z » : « 1 », « bar » : « 3 »}*, Add (Ajouter) définit les étiquettes pour cette adresse sur *{« foo » : « 1 », « z » : « 1 », « bar » : « 3 »}*.
- **Merge (Fusionner) :** Fusionne les étiquettes avec les adresses ou les sous-réseaux existants. Résout les conflits en sélectionnant des valeurs non vides sur les valeurs vides. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 », « qux », « corge » : « 4 »}* et que le fichier CSV contient *{ « z » : « 1 , « bar » : « », « qux » : « 3 », « corge : « 4-updated »}*, Merge (Fusionner) définit les étiquettes pour cette adresse à *{« foo » : "1 » , « z » : « 1« 1 »», « bar » : « 2 », « qux » : « 3 », « corge » : « 4-updated »}*.

  Note La valeur de « bar » dans n'est pas réinitialisée à « » (vide), au lieu de cela, la valeur existante de « bar » = « 2 » est conservée.

- **Delete (Supprimer) :** Cette option supprime les étiquettes pour une adresse ou un sous-réseau, ce qui peut avoir une incidence considérable sur les portées, les filtres, les politiques et le comportement appliqué. Pour obtenir des renseignements importants, consultez la section *Supprimer des étiquettes*.

Important : La fonction de suppression, lors du chargement des étiquettes personnalisées, supprimera TOUTES les étiquettes associées aux adresses IP ou aux sous-réseaux précisés, et ne se limitera pas aux colonnes répertoriées dans le fichier CSV. Par conséquent, l'opération Delete (Supprimer) doit être utilisée avec prudence.

Étape 4 Cliquez sur **Upload** (Téléverser).

Rechercher des étiquettes

Les utilisateurs ayant un rôle d' **administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent rechercher, afficher et modifier les étiquettes attribuées à une adresse IP ou à un sous-réseau.

Procedure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

Dans la page Assign Labels (Attribuer des étiquettes), les étiquettes existantes saisies pour l'adresse IP ou le sous-réseau sont affichées.

Attribuer ou modifier manuellement des étiquettes personnalisées

Les utilisateurs ayant le rôle d' **administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent affecter manuellement des étiquettes à une adresse IP ou à un sous-réseau donné.

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

La page Assign Labels (Affecter des étiquettes) s'affiche. Notez que les étiquettes existantes seront affichées et peuvent être modifiées.

Étape 3 Pour ajouter une nouvelle étiquette, dans la section **Étiquettes de <IP address/subnet>** , saisissez le nom et la valeur de l'étiquette, puis cliquez sur **Confirm** (Confirmer). Cliquez sur **Next** (suivant).

Étape 4 Passez en revue les modifications et cliquez sur **Assign** (Affecter) pour les valider.

Télécharger des étiquettes

Les utilisateurs ayant un rôle d' **administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée** racine peuvent télécharger des étiquettes précédemment définies appartenant à une portée racine.

Procedure

Étape 1 Dans la page **Label Management** (gestion des étiquettes), cliquez sur **User Defined Label Upload** (téléverser les étiquettes définies par l'utilisateur).

Étape 2 Dans la section **Download Existing Labels**(Télécharger les étiquettes existantes), cliquez sur **Download Labels** (Télécharger les étiquettes).

Les étiquettes utilisées par Cisco Secure Workload sont téléchargées dans un fichier CSV.

Modifier les étiquettes

Avertissement Si vous devez modifier une étiquette, faites-le avec prudence, car cela modifie les membres et les effets des requêtes, des filtres, des portées, des grappes, des politiques et du comportement appliqué existants qui reposent sur cette dernière.

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes), cliquez sur l'onglet **Search and Assign** (Rechercher et attribuer).

Étape 2 Dans le champ **IP or Subnet** (adresse IP ou sous-réseau), saisissez l'adresse IP ou le sous-réseau, puis cliquez sur **Next**(suivant).

Les étiquettes utilisées par Cisco Secure Workload pour l'adresse IP ou le sous-réseau saisi s'affichent.

Étape 3 Dans la colonne **Actions**, cliquez sur l'icône **Edit** (modifier) pour modifier le nom et la valeur de l'étiquette requise.

Étape 4 Cliquez sur **Confirm** (Confirmer) puis sur **Next**(suivant).

Étape 5 Passez en revue les modifications et cliquez sur **Assign** (Attribuer).

Désactiver les étiquettes

Une façon de modifier le schéma consiste à désactiver les étiquettes. *Procédez avec prudence*.

Procédure

Étape 1 Accédez à la page **Label Management** (gestion des étiquettes).

Étape 2 Pour l'étiquette requise, dans la colonne **Actions**, sélectionnez **Disable** (désactiver) et confirmez pour supprimer l'étiquette de l'inventaire en cliquant sur **Yes**(oui).

Si vous décidez ultérieurement d'activer l'étiquette, cliquez sur **Enable**(Activer) pour utiliser l'étiquette.

Supprimer des étiquettes

Avertissement Une façon de modifier le schéma consiste à désactiver les étiquettes et à les supprimer. Procédez avec prudence. Cette action supprime l'étiquette sélectionnée, ce qui a une incidence sur tous les **filtres** et toutes les **portées** qui en dépendent. Assurez-vous que ces étiquettes ne sont pas utilisées. Cette action ne peut pas être annulée.

Procédure

Étape 1 Désactivez les étiquettes. Consultez la section désactiver_étiquettes.

Étape 2 Cliquez sur l'icône de la **corbeille** et confirmez en cliquant sur **Yes** (oui) pour supprimer l'étiquette.

Afficher l'utilisation des étiquettes

L'inventaire des adresses IP ou des sous-réseaux est mis à jour avec les étiquettes personnalisées téléversées à l'aide de fichiers CSV ou attribuées manuellement par les utilisateurs. Les étiquettes sont ensuite utilisées pour définir les portées et les filtres, et les politiques d'application sont créées en fonction de ces filtres. Par conséquent, la compréhension de l'utilisation des étiquettes est essentielle, car toute modification apportée aux étiquettes a une incidence directe sur les portées, les filtres et les politiques de Cisco Secure Workload.

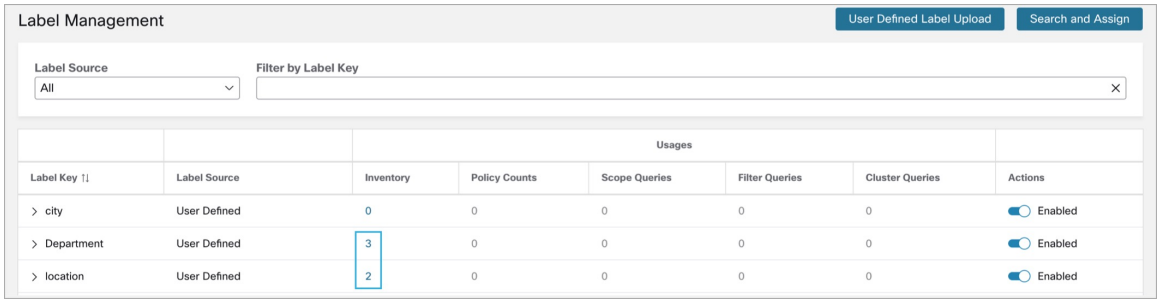
Pour afficher l'utilisation des étiquettes :

Procédure

Étape 1 Dans la page **Label Management** (Gestion des étiquettes) , les clés d'étiquette, les cinq principales valeurs des étiquettes utilisées, l'inventaire, les portées, les filtres et les grappes utilisant les étiquettes personnalisées sont affichés.

Étape 2 Dans la colonne Usages (utilisations), cliquez sur les valeurs de décompte de l'inventaire, des portées ou des filtres. Par exemple, pour afficher les portées à l'aide de l'étiquette « Location » (Emplacements), cliquez sur le nombre de requêtes sur la portée.

Illustration 177 : Afficher les portées de l'étiquette sélectionnée



La page Scopes and Inventory (Portées et inventaire) s'affiche et la requête filtre automatiquement les portées avec l'étiquette sélectionnée.

Remarque Vous pouvez uniquement afficher l'utilisation des étiquettes téléversées à l'aide de fichiers CSV ou attribuées manuellement à l'adresse IP ou au sous-réseau.

Créer un processus pour la tenue des étiquettes

Votre réseau et votre inventaire changeront, et vous devez planifier de mettre à jour les étiquettes pour refléter ces changements.

Par exemple, si une charge de travail est supprimée et que son adresse IP est réaffectée à une charge de travail avec un objectif différent, vous devez mettre à jour les étiquettes associées à cette charge de travail. Cela est vrai pour les étiquettes téléversées manuellement et pour les étiquettes conservées dans d'autres systèmes et acquises à partir d'autres systèmes, comme une base de données de gestion de configuration (CMDB).

Créez un processus pour vous assurer que vos étiquettes sont mises à jour régulièrement et en permanence, et ajoutez ce processus à votre routine d'entretien du réseau.

Portées et inventaire

Aperçu de la portée et de l'inventaire

Cette section permet de visualiser la hiérarchie de la portée, ainsi que tout l'inventaire qu'elle contient. Les portées classent l'ensemble de l'inventaire selon une structure hiérarchique. Consultez Inventory, on page 349. Sur la gauche se trouve l'interface utilisateur du répertoire de la portée. Ici, vous pouvez parcourir votre hiérarchie de portée. Chaque portée est affichée dans une carte de portée. Elle affiche le nom de la portée, le nombre de portées enfants, le décompte de l'inventaire et, le cas échéant, l'inventaire non catégorisé. Cliquer sur une carte de portée met à jour le volet de droite pour afficher les détails de cette portée ainsi qu'une liste filtrable de tout son inventaire.

Principes de conception de la portée

1. L'inventaire est apparié à l'arborescence de la portée en fonction de la correspondance de requête dynamique.
   - Les requêtes peuvent correspondre à l'adresse IP ou au sous-réseau, ou à l'étiquette (option préférée)
   - L'arbre est formé grâce à des requêtes conjuguées à chaque couche.
2. La structure de la portée peut être propre à l'emplacement, le cas échéant.
   - Nuage combiné contre Centre de données et Nuage spécifique contre Emplacement géographique
3. Chaque couche de l'arborescence de portée doit constituer un point d'ancrage pour le :
   - Contrôle des politiques
   - Contrôle d'accès en fonction des rôles (RBAC)
4. Chaque portée enfant doit être un sous-ensemble de sa portée parente.
   - Assurez-vous que les portées ne se chevauchent pas, voir Chevauchement de portée

Note Chaque organisation est structurée différemment et, selon votre secteur d'activité, nécessite des approches différentes. choisir un objectif lors de la conception de votre hiérarchie de portée; l'emplacement, l'environnement ou l'application.

Note N'utilisez pas d'adresse IP ou de sous-réseau pour définir des portées qui impliquent l'inventaire Kubernetes. Vous devez utiliser des étiquettes pour définir la portée et la politique pour ces charges de travail. L'adresse IP seule n'est pas suffisante pour identifier les services de pods; l'utilisation de l'adresse IP pour la définition de la portée produira des résultats non fiables.

Principales caractéristiques

La fonction de filtrage pour les portées et l'inventaire vous permet de parcourir rapidement l'arborescence des portées ou de filtrer la hiérarchie des portées et les éléments d'inventaire de la portée sélectionnée.

Le décompte de l'inventaire est affiché dans la carte des portées, ce qui permet de voir rapidement le nombre de charges de travail dans la portée.

Portées

Les portées sont un élément essentiel de la configuration et des politiques dans Cisco Secure Workload. Les portées constituent un ensemble de charges de travail organisées selon une hiérarchie. Les charges de travail étiquetées pour servir d'attributs qui construisent un modèle sur leur emplacement, leur rôle et leur fonction dans votre environnement. Les portées fournissent une structure pour prendre en charge des mécanismes dynamiques comme l'identification et les attributs associés à une adresse IP qui peuvent évoluer avec le temps.

Les portées sont utilisées pour regrouper les applications de centre de données et, avec les Rôles, elles permettent un contrôle précis de leur gestion. Par exemple, les portées sont utilisées sur l'ensemble du produit pour définir l'accès aux Gérer le cycle de vie des politiques dans Cisco Secure Workload, on page 429, aux Flux de réseau – Visibilité du trafic et aux Filtres.

Les portées sont définies hiérarchiquement comme des ensembles d'arborescences, la racine correspondant à un **VRF**. Par conséquent, chaque hiérarchie d'arborescence de portée représente des données disjointes qui ne se chevauchent pas avec une autre arborescence de portée, voir la section Chevauchement de portée.

Définition de la portée

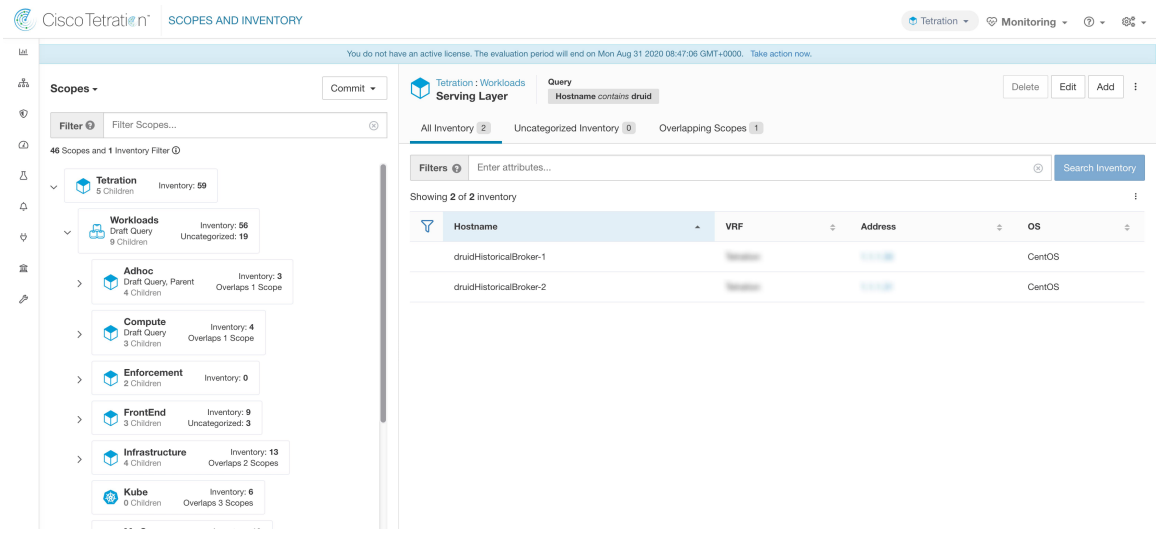
Chaque portée est définie par les attributs ci-dessous :

Attribut	Description
Portée parente	Le parent de la nouvelle portée définit la structure hiérarchique de l'arborescence.
Nom	Le nom pour identifier la portée.
Type	Utilisé pour spécifier différentes catégories d'inventaire. Si aucun n'est applicable, ou si la portée contient une combinaison, ce champ peut être laissé vide.
Requête	La requête définissant la portée individuelle.

Note Les portées doivent être définies dans une hiérarchie qui imite la hiérarchie de propriété des applications de l'organisation.

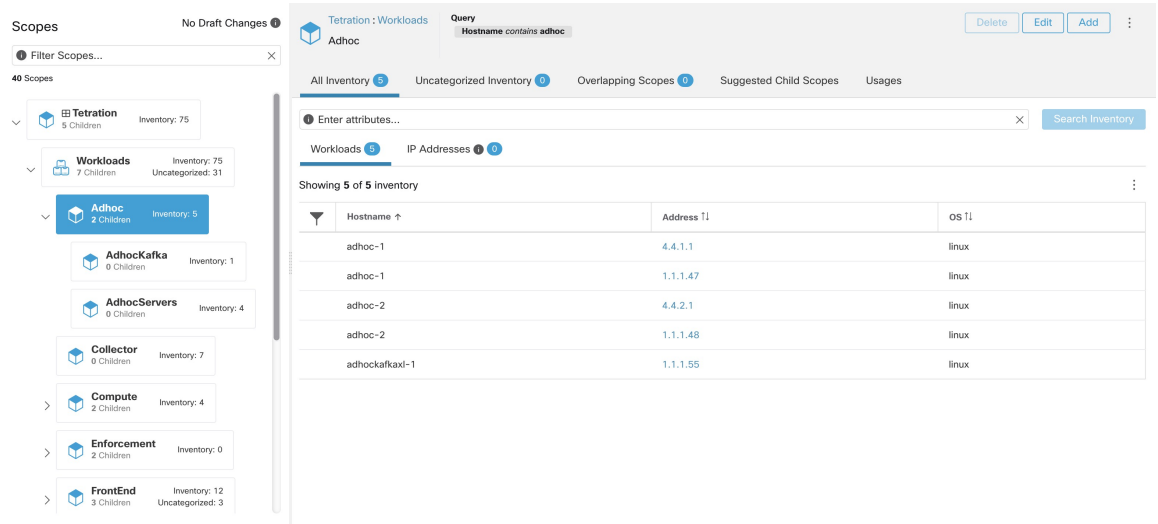
Note La requête peut correspondre à l'adresse IP du sous-réseau ou à d'autres attributs de l'inventaire.

Figure 178: Exemple de navigation dans la hiérarchie des portées



Le répertoire des portées affiche la hiérarchie des portées et certains détails de chaque portée (par exemple, le nombre d'inventaires, le nombre de portées enfants, les espaces de travail). Cliquez sur une portée pour la sélectionner, et le volet d'informations à droite se met à jour avec plus d'informations sur cette portée et l'inventaire de cette dernière.

Figure 179: Inventaire



Filtre de portée

Les utilisateurs peuvent utiliser le filtre Portée pour identifier rapidement différents détails de portée tels que les portées et les requêtes qui se chevauchent. La fonction de filtre est également utile pour identifier les modifications de requête, les modifications de parent, etc.

Champ	Description
Nom	Filtrer par le nom de la portée ou du filtre d'inventaire.

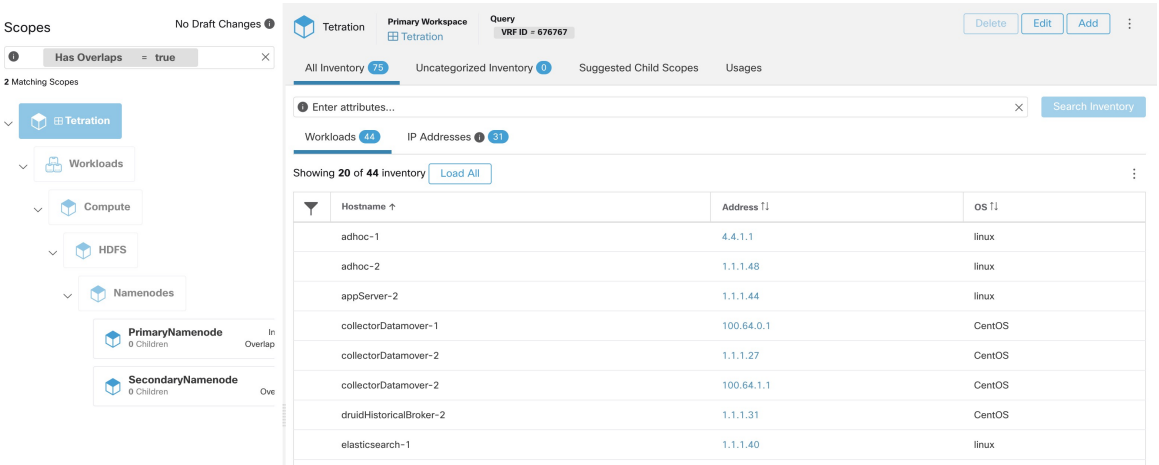
Champ	Description
Description	Filtrer en fonction du texte figurant dans la description d'une portée.
Requête	Filtrer par champs ou valeurs utilisés dans la requête.
Changement de requête	Filtrer par portées qui ont une requête non validée.
Changement de parent	Filtrer par portées qui ont été déplacées dans le brouillon mais non validées.
Est-ce un filtre d'inventaire?	Affichez les filtres d'inventaire limités à leur portée de propriété.
Possède un espace de travail	Filtrez par portées qui ont un espace de travail principal.
Possède un espace de travail appliqué	Filtrer par portées qui ont un espace de travail principal appliqué.
A des chevauchements	Filtrer par portées qui ont un inventaire en commun avec une portée connexe.
A une requête non valide	Filtrez par portées dont la requête utilise des étiquettes non valides ou inconnues.

Exemples :

A des chevauchements

Exemple de chevauchement de portée

Figure 180: A des chevauchements

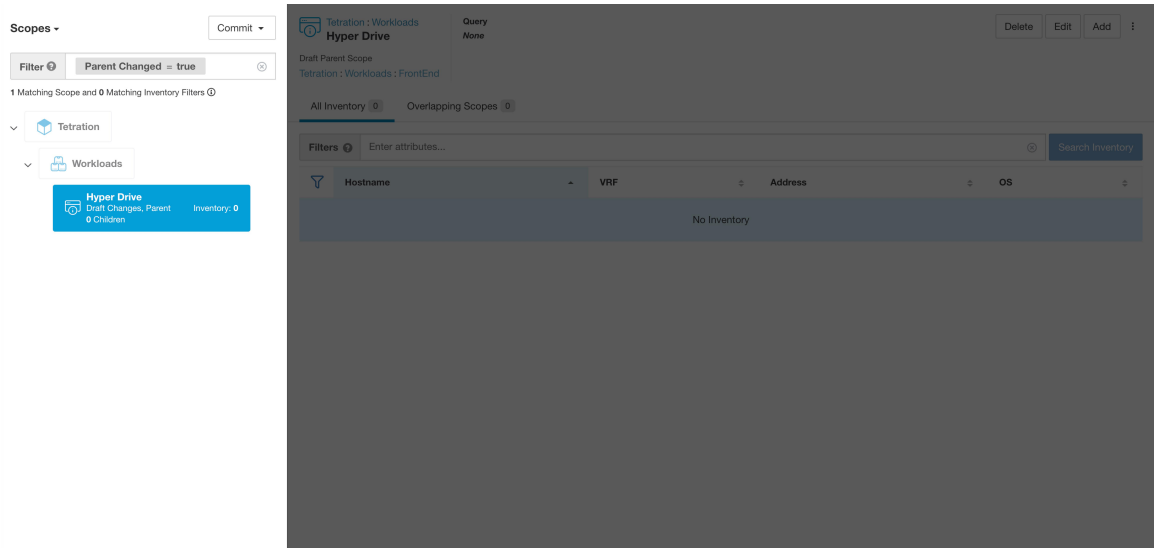


Pour en savoir plus, consultez Chevauchement de portée.

Changement de parent

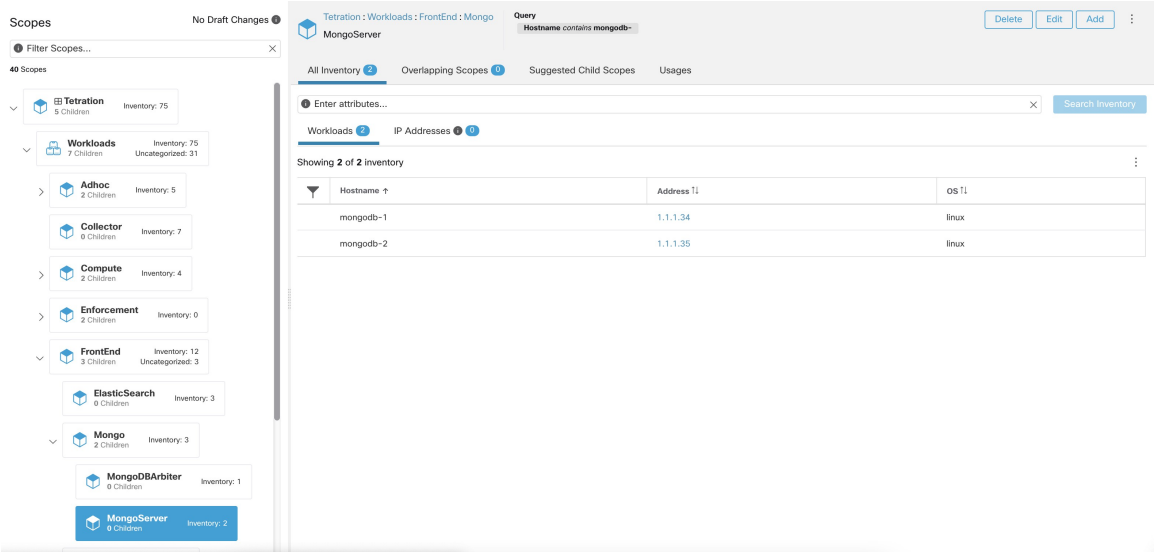
Les portées ont été déplacés dans le brouillon, mais pas encore validés.

Figure 181: Changement de parent



Requêtes de portée complète

Figure 182: Exemple de hiérarchie de portée



Les portées sont définies hiérarchiquement, la requête complète de la portée est définie comme le « et » logique de la portée avec tous ses parents. En utilisant l'exemple ci-dessus, les ressources affectées à `Workloads:FrontEnd:Mongo`

La portée correspondrait à :

```
vrf_id = 676767 and (ip in 1.1.1.0/24) and (Hostname contains mongo).
```

Où vrf_id = 676767 provient de la requête de portée racine et IP dans 1.1.1.0/24 de la requête de portée parente.

Note Il est conseillé de ne pas avoir des requêtes qui se chevauchent au même niveau. Cela supprime l'importance de l'ordre et réduit la confusion. Voir Chevauchement de portée

Fourniture de l'accès aux portées

Vous pouvez accorder les capacités de lecture, d'écriture, de mise en application et de propriétaire sur les portées. Pour en savoir plus, consultez la section sur les **rôles** dans le *Guide de l'utilisateur de Cisco Secure Workload*.

Un utilisateur a accès à une « sous-arborescence ». C'est-à-dire à une portée donnée et tous ses enfants. Dans l'exemple précédent, vous avez l'accès en lecture à la portée `Workloads:FrontEnd` et auriez, par héritage, accès en lecture à toutes les portées sous `Workloads:FrontEndl`, y compris :

- `Workloads:FrontEnd:Mongo`
- `Workloads:FrontEnd:ElasticSearch`
- `Workloads:FrontEnd:Redis`
- `etc. . .`

Il est possible de définir des rôles avec un accès à plusieurs portées. Par exemple, un rôle « Administrateur Mongo » pourrait avoir un accès Propriétaire aux portées :

- `Workloads:FrontEnd:Mongo:MongoServer`
- `Workloads:FrontEnd:Mongo:MongoDBArbiter`

Les rôles et les capacités vous permettent d'avoir un accès horizontal à la hiérarchie de la portée.

Les capacités de portée sont également héritées. Par exemple, avoir la capacité d'écriture sur une portée permet également de lire ces informations.

Affichage des portées

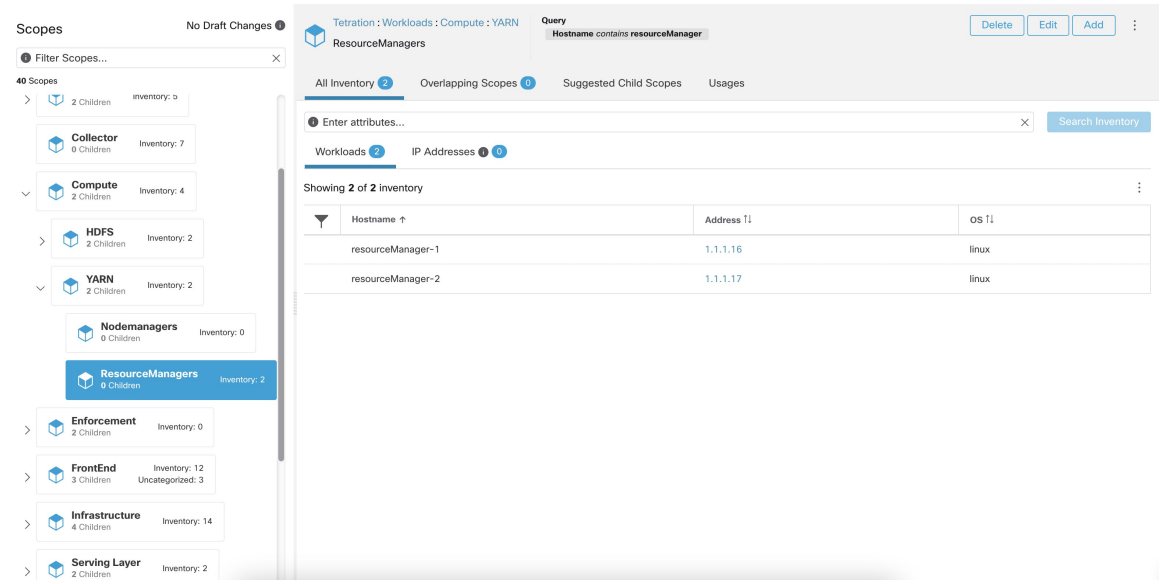
Chaque utilisateur peut afficher l'arborescence de portées à laquelle il a accès. Les utilisateurs qui ont le droit de propriétaire sur la portée racine ont la possibilité de créer, de modifier et de supprimer une portée dans cette arborescence. Pour accéder à cet affichage :

Dans la barre de navigation de gauche, cliquez sur **Organize (Organiser)** > **Scopes and Inventory (Portées et inventaire).**

Vous pouvez parcourir la hiérarchie complète des portées (jusqu'à la racine) pour toutes les portées auxquelles vous avez accès. Ce parcours complet fournit un contexte, car les utilisateurs peuvent créer des politiques pour n'importe quelle portée. Plusieurs actions peuvent être effectuées sur cette page :

- Cliquez sur le chevron dans la hiérarchie de la portée pour afficher les enfants de cette portée.
- En cliquant sur la carte de la portée, le volet de droite s'actualise et affiche les détails de cette portée ainsi qu'une liste filtrable de l'ensemble de son inventaire.

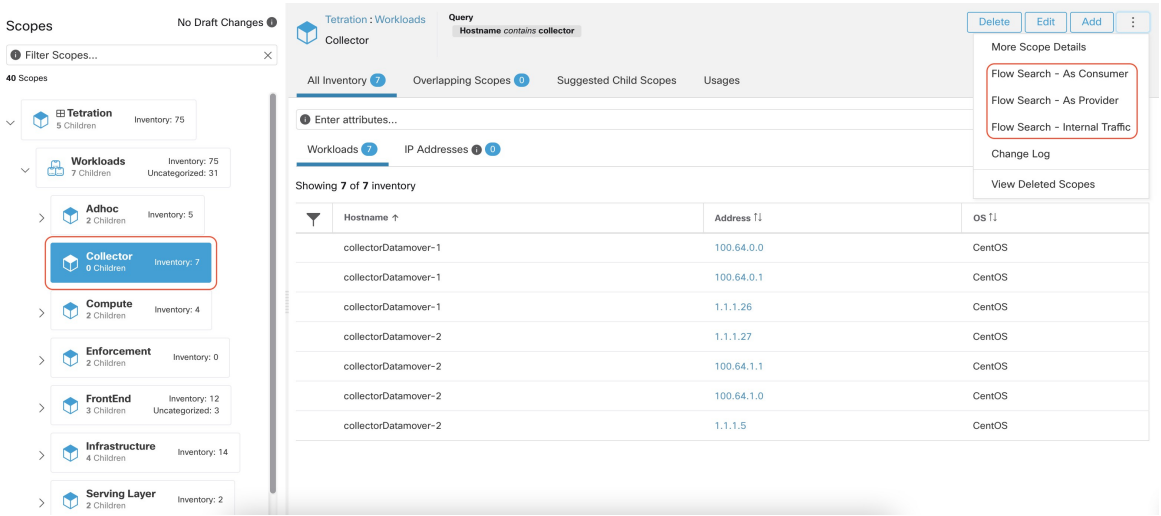
Figure 183: Exemple d'affichage non administrateur



Recherche de flux faisant référence à une portée

Des raccourcis sont proposés sur la page des portées pour aider l'utilisateur dans les scénarios où il doit rechercher des flux dont l'un ou les deux points terminaux se situent dans une portée donnée.

Figure 184: Recherche de flux pour une portée



Après avoir sélectionné la portée souhaitée dans l'arborescence (panneau de gauche), comme le montre la figure ci-dessus, l'utilisateur peut choisir entre les trois options suivantes :

1. *Recherche de flux en tant que consommateur* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux avec la portée sélectionnée comme portée de *consommateur* pour les flux. En d'autres termes, le point terminal consommateur ou source dans les flux appartient à la portée sélectionnée.

2. *Recherche de flux en tant que fournisseur* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux avec la portée sélectionnée comme portée du *fournisseur* pour les flux. Autrement dit, le fournisseur ou le point terminal de destination dans les flux appartient à la portée sélectionnée.
3. *Recherche de flux de trafic interne* fournit un raccourci vers la page de recherche de flux pour aider à rechercher des flux qui sont complètement limités à la portée sélectionnée. En d'autres termes, les deux points terminaux des flux (le client et le fournisseur) appartiennent à la portée sélectionnée.

Création d'une nouvelle portée

Les portées enfants sont créées sur la page d'administration **Scopes** (Portées). Cette action nécessite la capacité `SCOPE_OWNER` (PROPRIÉTAIRE_PORTÉE) sur la portée racine.Les **administrateurs de site** sont propriétaires de toutes les portées.

La création d'une portée enfant aura une incidence sur les membres à l'inventaire de l'application (charges de travail membres) de la portée parente. Par conséquent, la portée parente sera marquée comme ayant des « modifications en cours ». Les modifications devront être validées, et les structures tributaires devront être mises à jour. Reportez-vous à Valider les modifications.

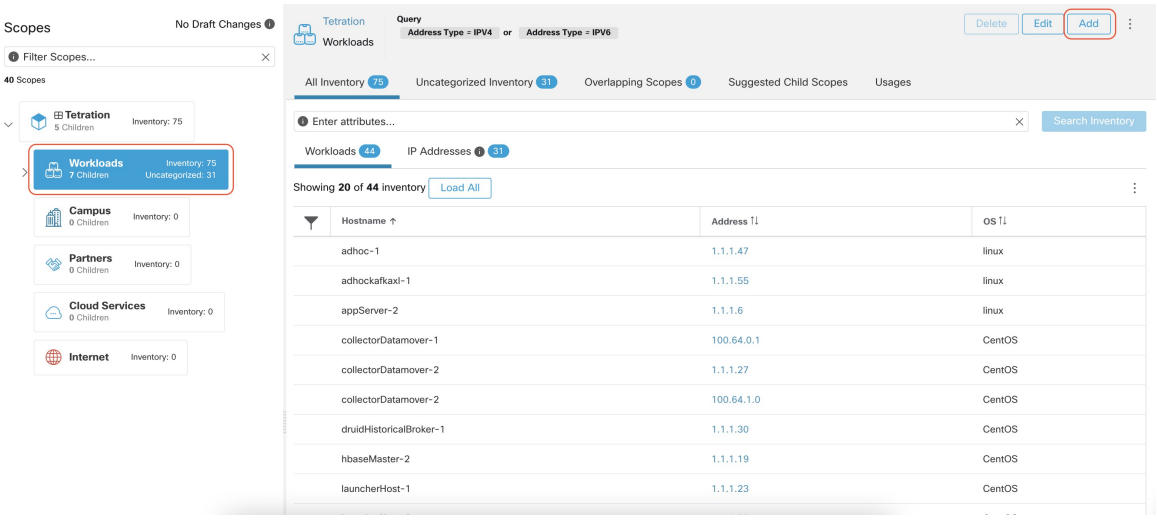
Procedure

Étape 1 Dans la barre de navigation de gauche, cliquez sur **Organize (Organiser)** > **Scopes and Inventory (Portées et inventaire).** La page affiche les portées racine correspondant aux détenteurs + VRF déjà créés sur le système.

Étape 2 Sélectionnez une portée enfant dans le répertoire des portées. Vous pouvez d'abord filtrer les portées si nécessaire.

Étape 3 Cliquez sur le bouton **Add** (ajouter).

Figure 185: Bouton Ajouter une portée

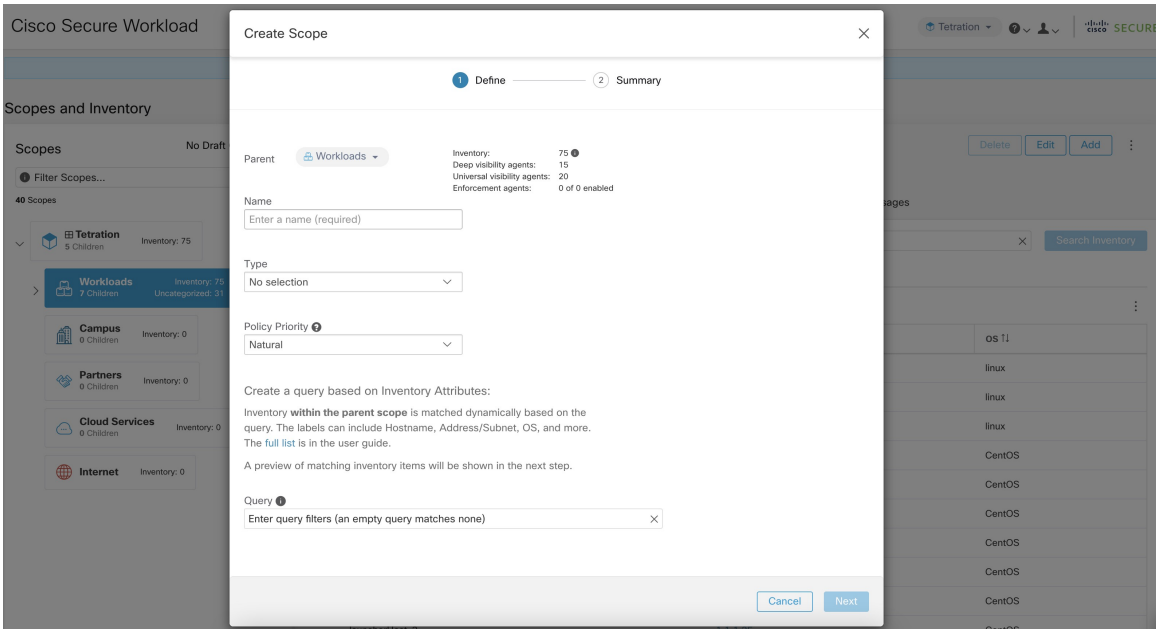


Étape 4 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Parents	Le parent de la nouvelle portée.

Champ	Description
Nom	Le nom pour identifier la portée. Doit être unique dans la portée parente
Type	Sélectionnez une catégorie pour la nouvelle portée.
Requête	La requête/le filtre à mettre en correspondance avec les ressources.

Figure 186: Boîte de dialogue modale de création de portée

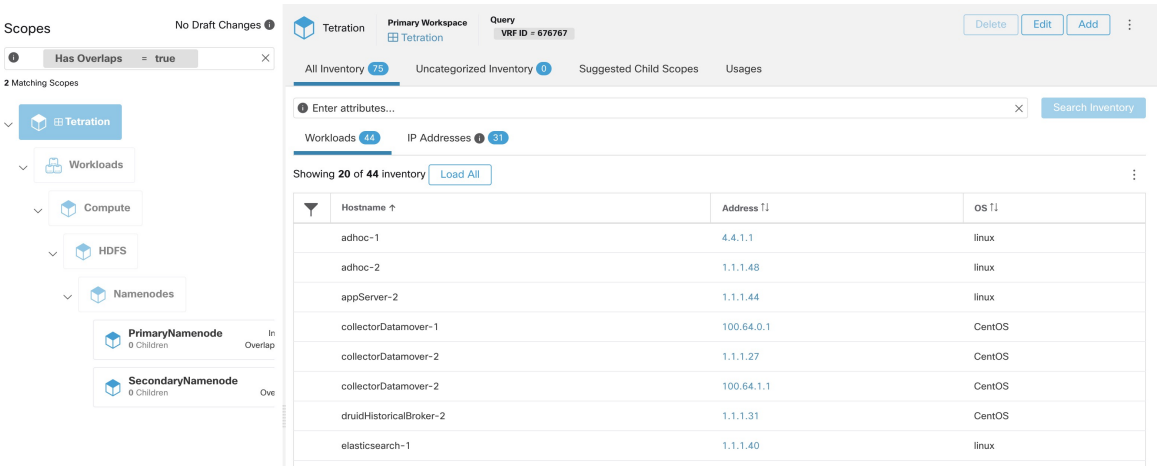


Chevauchement de portée

Lors de l'ajout de portées, il est recommandé d'éviter le chevauchement des portées. Lorsque les portées se chevauchent, les politiques générées pour les portées qui se chevauchent peuvent potentiellement créer de la confusion chez les utilisateurs finaux. Cette fonctionnalité avise l'utilisateur de manière proactive en cas de chevauchement d'appartenances à des portées, c'est-à-dire si le même inventaire appartient à plusieurs portées à la même profondeur dans l'arborescence des portées (portées jumelles). L'objectif est d'éviter que la même charge de travail se trouve dans différentes parties de l'arborescence de la portée.

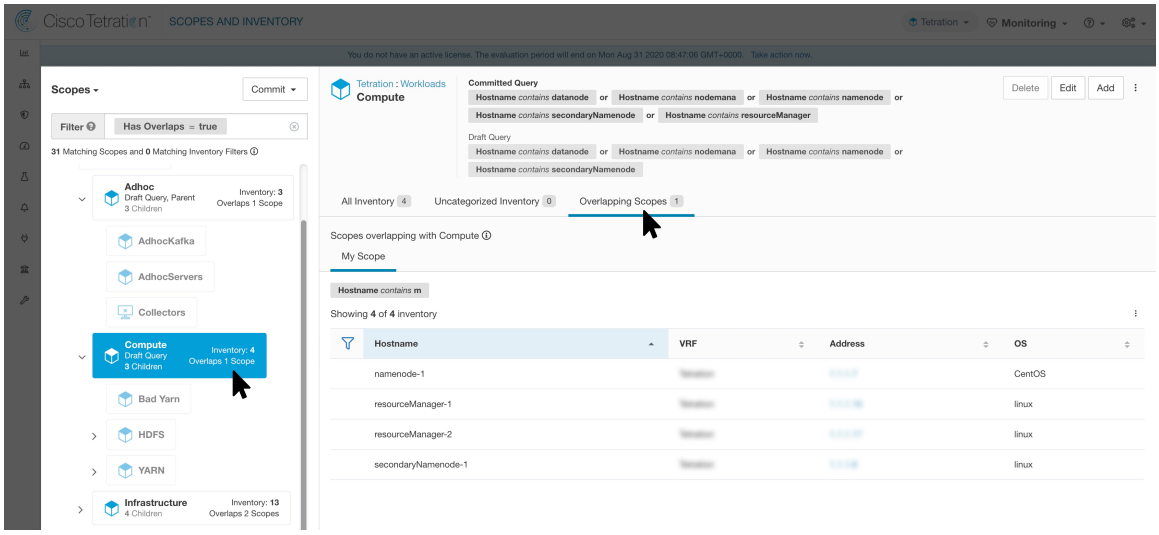
Pour afficher les éléments de l'inventaire appartenant à plusieurs portées, utilisez le filtre de portée et saisissez le critère **Has Overlaps = vrai**.

Figure 187: Critère de chevauchement dans le filtre de portée



La liste des portées qui se chevauchent et des adresses IP qui se chevauchent correspondantes peut être consultée en parcourant l'arborescence de la portée et en sélectionnant l'onglet **Overlapping Scopes** (portées en chevauchement).

Figure 188: Chevauchement des portées et des adresses IP



Modification des portées

Les portées peuvent uniquement être modifiées par les utilisateurs ayant la capacité `SCOPE_OWNER` (Propriétaire de portée) sur la portée racine. Les administrateurs de site sont propriétaires de toutes les portées.

Modification d'un nom de portée

La modification d'un nom de portée se produit immédiatement et peut prendre plusieurs minutes en fonction du nombre de portées enfants à mettre à jour.

Note Les recherches de flux par nom de portée seront affectées lors de la modification du nom de la portée.

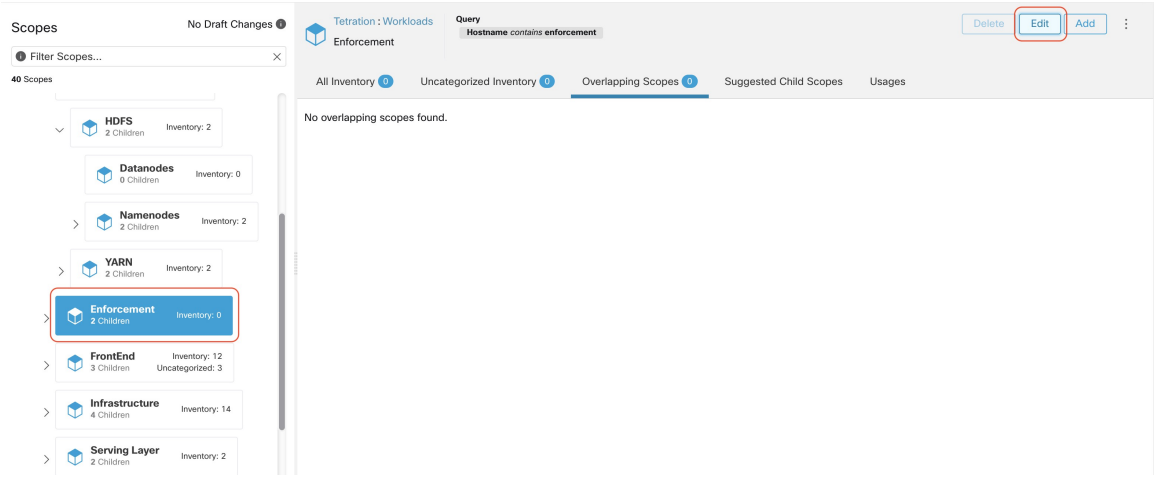
Modification d'une requête de portée

Lorsqu'une requête de portée est modifiée, les portées parentes et enfant directes sont touchées. Ces portées sont marquées comme ayant des « modifications en cours » indiquant que des modifications ont été apportées à l'arborescence qui n'ont pas été validées. Une fois que toutes les mises à jour des requêtes ont été effectuées, l'utilisateur doit cliquer sur le bouton **Commit Changes** (Valider les modifications) au-dessus du répertoire de la portée pour rendre la modification permanente. Cela déclenchera une tâche en arrière-plan pour mettre à jour toutes les requêtes de portée et les « requêtes de grappe dynamique » dans l'espace de travail.

Warning La mise à jour d'une requête de portée peut avoir une incidence sur les membres de l'inventaire des portées (les charges de travail qui sont membres de la portée). Les modifications prendront effet pendant le processus de **validation des modifications**. Pour atténuer les risques, vous pouvez comparer les changements d'affiliation pour une analyse d'impact plus approfondie à partir de la fenêtre Examiner l'incidence des modifications de la portée/du filtre (Examiner la portée/l'impact des changements de filtre).

De nouvelles règles de pare-feu d'hôte seront insérées et toutes les règles existantes seront supprimées sur les hôtes concernés.

Figure 189: Modifier une portée



Pour modifier une portée :

Procedure

Étape 1 Cliquez sur le **bouton Edit**) (Modifier) de la portée à modifier.

Étape 2 Modifiez le nom ou la requête pour la portée sélectionnée.

Étape 3 Comparez les modifications entre l'ancienne et la nouvelle requête provisoire en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête).

Étape 4 Cliquez sur **Save** (enregistrer). Le nom est mis à jour immédiatement.

Étape 5 Pour mettre à jour la requête de toutes les portées, cliquez sur le bouton **Commit Changes** (Valider les modifications).

Étape 6 Vous obtiendrez une confirmation contextuelle qui indiquera les conséquences de la modification de la portée. La mise à jour est traitée de manière asynchrone dans une tâche en arrière-plan.

Étape 7 Cliquez sur **Save** (enregistrer). Selon le nombre de modifications, l'opération peut prendre une minute ou plus.

Figure 190: Examiner l'incidence de la modification de la requête

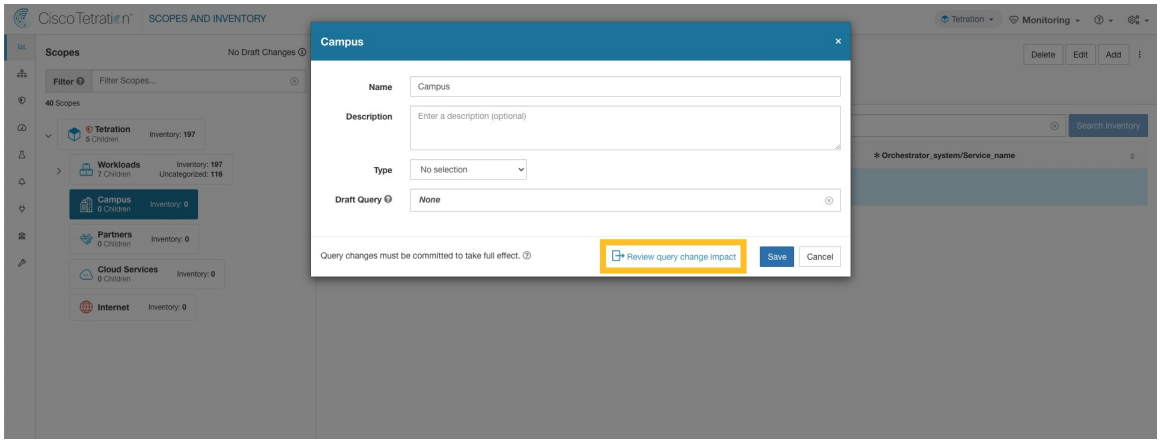
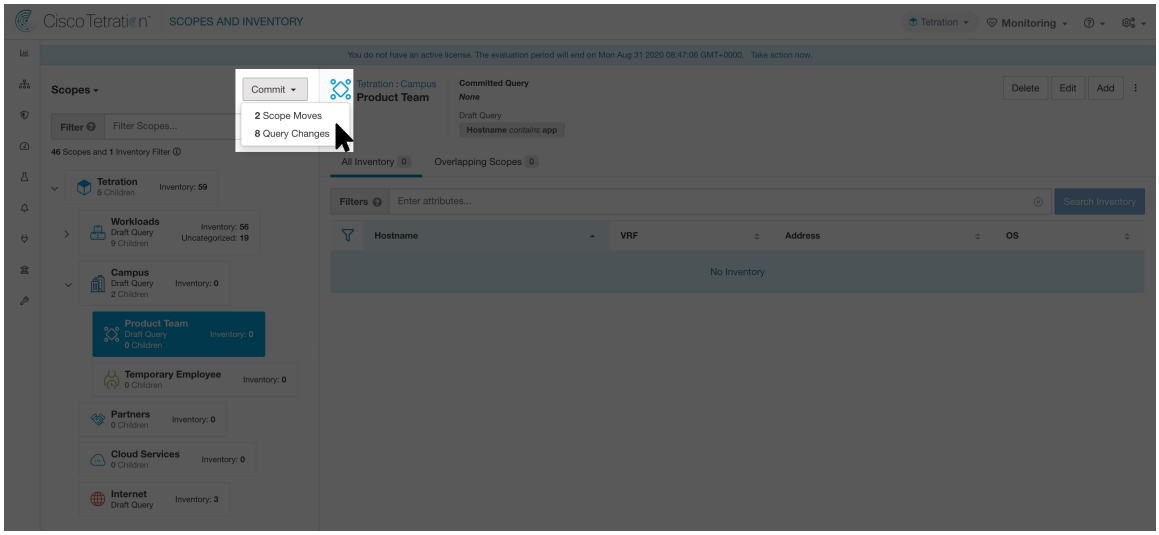


Figure 191: Valider les modifications



Modification du parent d'une portée

Lorsque le parent d'une portée est mis à jour, la requête de portée change. Cette modification affecte les membres des portées parent et enfant. Tout comme la modification de la requête de portée, ces modifications sont initialement enregistrées en tant que « brouillons de modifications » et n'entreront en vigueur que si elles sont validées. L'utilisateur peut valider l'incidence de cette modification avant de s'engager en cliquant sur « Revoir la requête de modification de l'impact » dans la boîte de dialogue modale Edit Scope (modifier la

portée). Une fois validées, les modifications peuvent être validées en cliquant sur « Commit » (Valider) et en acceptant les « déplacements de la portée » et les « modifications de requêtes ».

Pour modifier le parent d'une portée :

Procedure

Étape 1 Cliquez sur le **bouton Edit**) (Modifier) de la portée à modifier.

Étape 2 Modifiez le parent de la portée sélectionnée.

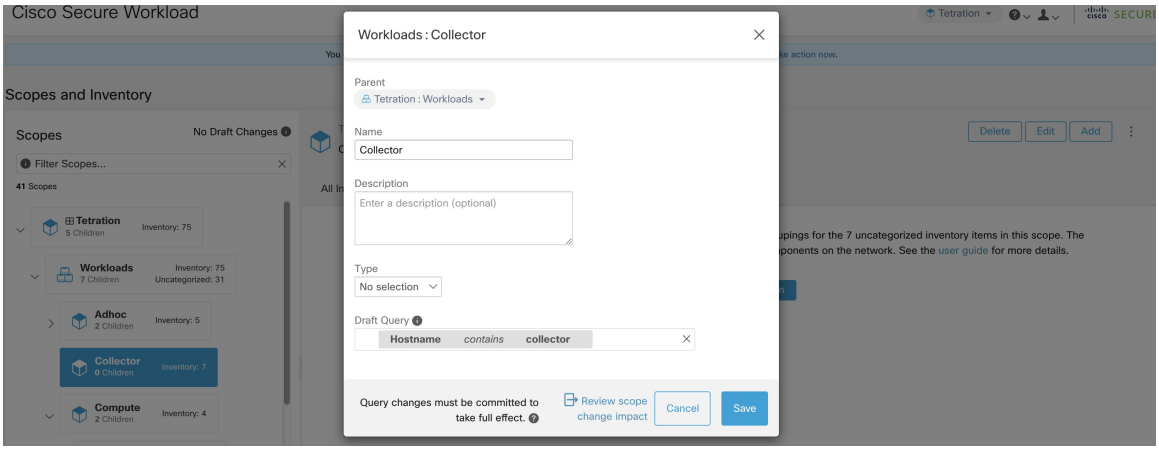
Étape 3 Comparez les modifications entre l'ancienne et la nouvelle version provisoire de la requête en cliquant sur le lien **Examiner l'incidence des modifications de la requête**.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Cliquez sur « Commit » (valider) et acceptez les « déplacements de portée » et les « modifications de requête ». La mise à jour est traitée de manière asynchrone dans une tâche en arrière-plan.

Étape 6 Cela peut prendre une minute ou plus selon le nombre de charges de travail concernées par cette modification.

Figure 192: Modification de la portée parente de la portée par défaut à Default:ProdHosts



Suppression des portées

Les portées peuvent uniquement être supprimées par les utilisateurs avec la capacité `SCOPE_OWNER` sur la portée racine. Les administrateurs de site sont propriétaires de toutes les portées.

La suppression d'une portée aura une incidence sur les membres de l'inventaire des applications de la portée parente (les charges de travail qui sont membres de la portée parente). . Par conséquent, la portée parente sera marquée comme ayant des « modifications en cours ». Les modifications devront être validées, et les structures tributaires devront être mises à jour. Reportez-vous à Valider les modifications.

Les portées avec des objets dépendants ne peuvent pas être supprimées. Une erreur est renvoyée si :

- Un espace de travail est défini pour la portée.
- Un filtre d'inventaire est affecté à la portée.
- Il existe une politique qui utilise la portée pour définir ses consommateurs ou ses fournisseurs.

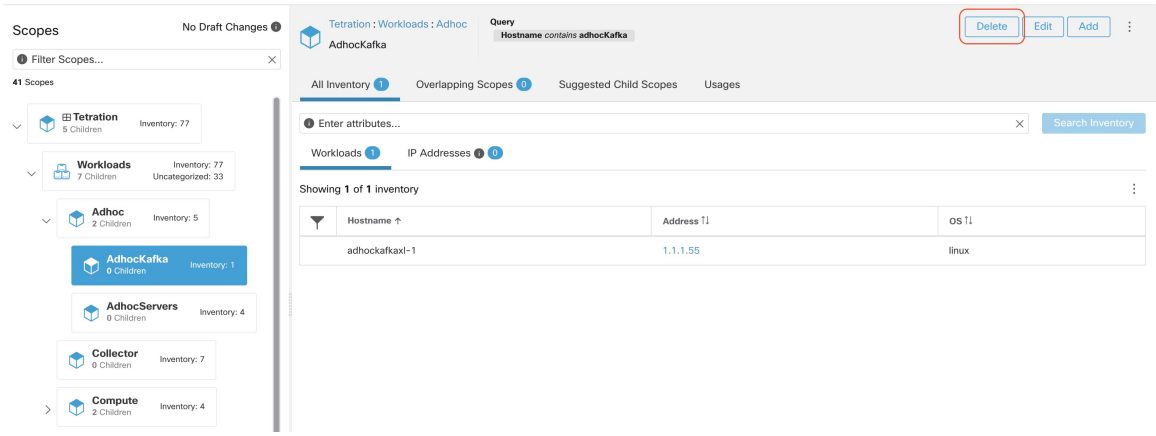
- Un intent (action associée des données) de configuration d'agent est défini sur la portée
- Un intent de configuration d'interface est définie sur la portée.
- Un intent de configuration de criminalistique est définie sur la portée.

Pour approfondir davantage les dépendances de la portée, vous pouvez consulter l'onglet **Dependencies** 'Dépendances) dans la fenêtre Examiner l'incidence des modifications de la portée/du filtre (Examiner la portée/l'impact des modifications de filtre).

Ces objets doivent être supprimés avant que la portée ne puisse être supprimée.

1. Dans le menu de navigation de gauche, choisissez **Organize (Organiser)** > **Scopes and Inventory (Portée et inventaire)**.
2. Sélectionnez une « portée », puis cliquez à nouveau pour afficher les portées enfants. Sélectionnez la portée enfant que vous souhaitez supprimer.
3. Cliquez sur le bouton **Delete** (Supprimer) à côté des boutons de modification et d'ajout.

Figure 193: Supprimer une portée



Note Seules les portées sans enfant peuvent être supprimées

Note Les portées racine doivent être supprimées en retirant le VRF (Virtual Routing and Forwarding, Instance virtuelle de routage et de transmission) de la page Tenants (Détenteurs).

Réinitialiser l'arborescence des portées

Si l'une des configurations ci-dessus existe, vous devez la supprimer avant de pouvoir réinitialiser l'arborescence de la portée. Tant que vous ne le faites pas, le bouton Reset (réinitialiser) n'est pas disponible.

Pour réinitialiser l'arborescence de la portée :

Avant de commencer

Vous pouvez supprimer l'ensemble de l'arborescence de la portée et recommencer.

La réinitialisation de l'arborescence des portées supprime toutes les portées, les étiquettes, les espaces de travail et les règles de collecte. Elle ne supprime pas les données intégrées/acquises (ingested).

Seul un utilisateur avec la capacité `SCOPE_OWNER` sur la portée racine peut réinitialiser l'arborescence de la portée.

Cependant, vous ne pouvez pas réinitialiser l'arborescence des portées si l'une des conditions suivantes est définie pour une portée de l'arborescence :

- Espaces de travail (à l'exception de l'espace de travail unique créé si vous avez créé l'arborescence de la portée à l'aide de l'assistant)
- Filtres d'inventaire
- Politiques
- Intents de configuration de l'agent
- Intents de configuration d'interface
- Intents de configuration criminalistique

Procédure

Étape 1 Dans le menu de navigation de gauche, choisissez **Organize (Organiser)** > **Scopes and Inventory (Portée et inventaire).**

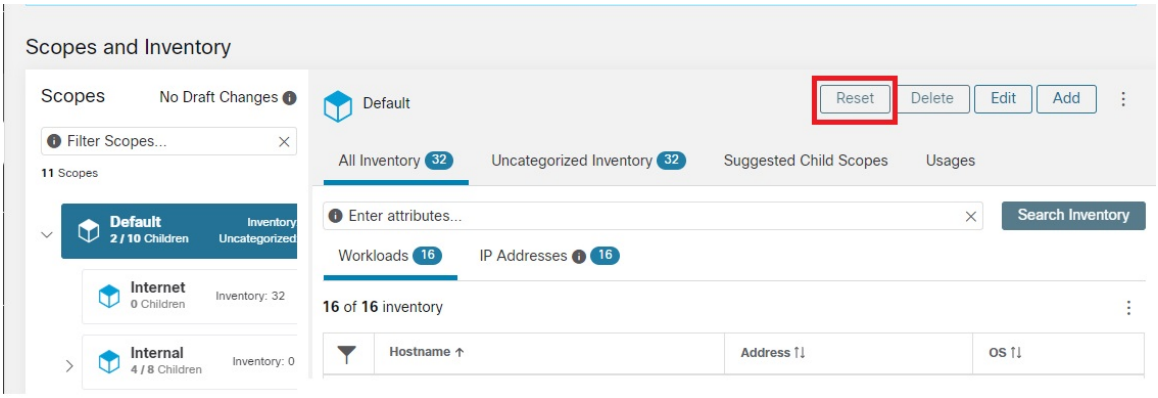
Étape 2 Cliquez sur la portée au sommet de l'arborescence.

Étape 3 Cliquez sur **Reset** (Réinitialiser).

Étape 4 Confirmez votre choix.

Étape 5 Si nécessaire, actualisez la page du navigateur pour continuer.

Illustration 194 : Réinitialiser l'arborescence de la portée



Valider les modifications

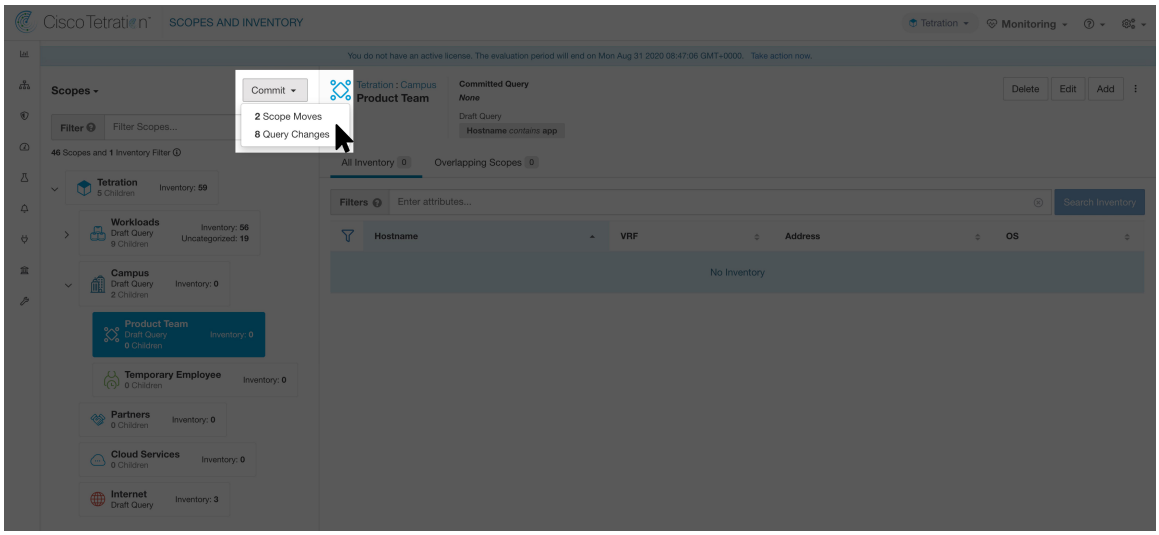
La définition de requête d'inventaire des applications d'une portée est définie par sa requête et celles de ses portées enfants directes. Lorsque cela se produit, la portée est marquée comme ayant des « modifications au stade du brouillon et non validées » et la requête, les espaces de travail et les grappes de la portée ne seront pas modifiés tant que la tâche en arrière-plan de**Commit Changes** (Valider les modifications) ne sera pas exécutée. Lorsqu'une portée est à l'état de brouillon, le symbole triangulaire d'avertissement est affiché à côté des icônes des portées concernées, et le bouton « Commit Changes » (valider les modifications) est affiché sur la page des portées (en haut à droite) et doit être pressé pour exécuter la tâche en arrière-plan **Valider les modifications**.

Événements qui peuvent marquer une portée comme au stade du brouillon :

- Mise à jour de la requête
- La requête de toute portée parent est mise à jour.
- Une portée enfant directe est ajoutée.
- Un enfant direct est supprimé.
- La requête directe de la portée enfant est mise à jour.

La modification du nom d'une portée ne modifie pas l'état de brouillon de la portée.

Figure 195: Valider les modifications



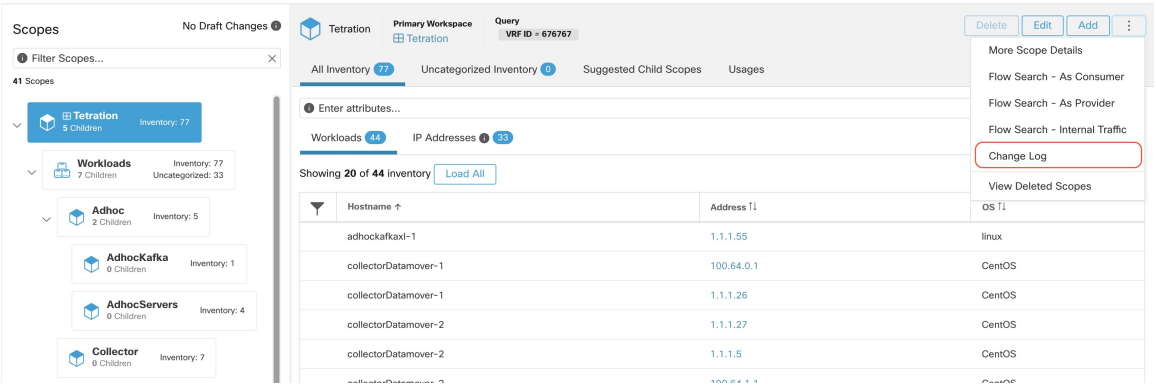
Note La tâche **Valider les modifications** est asynchrone. Elle prend généralement plusieurs secondes, mais les arborescences de portées volumineuses peuvent prendre plusieurs minutes.

Note La tâche de mise à jour de la portée sera terminée lorsque la portée racine ne sera plus à l'état de brouillon. Actualisez la page pour obtenir le dernier état.

Journal des modifications

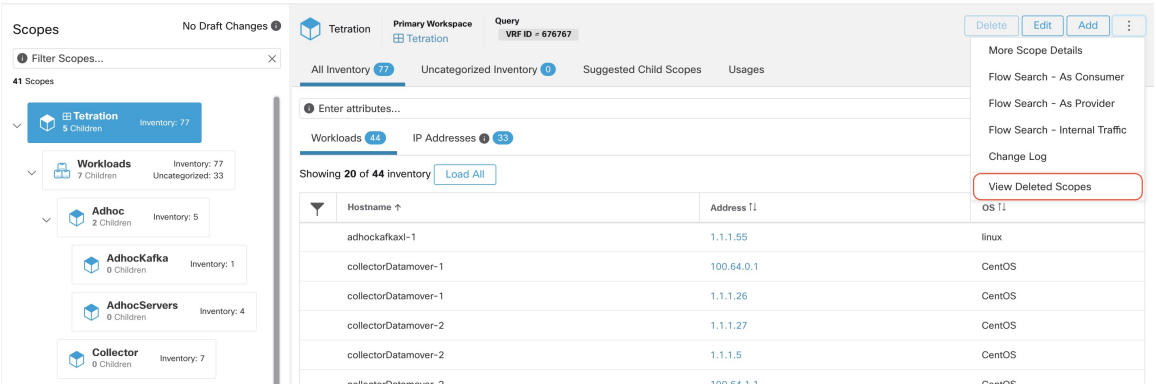
Les **administrateurs du site** et les utilisateurs avec la capacité `SCOPE_OWNER` sur la portée racine peuvent afficher les journaux des modifications pour chaque portée en cliquant sur change log (journal des modifications) dans le menu à développer en haut à droite.

Figure 196: Journal des modifications



Ces utilisateurs peuvent également afficher une liste des portées supprimées en cliquant sur le lien **View Deleted Scopes** (Afficher les portées supprimées) dans le menu à développer dans le coin supérieur droit.

Figure 197: Afficher les portées supprimées



Création d'un nouveau détenteur

Les portées au niveau racine sont mappées aux VRF qui sont créés sous les détenteurs ou par le biais de la page d'administration des **portées**. Cette action est uniquement disponible pour les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **Tenants (Détenteurs).**

Étape 2 Cliquez sur le bouton **Create New Tenant** (Créer un nouveau détenteur).

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Le nom pour identifier la portée. Doit être unique dans la portée parente
Description	Description facultative

Étape 4 Cliquez sur le bouton **Create** (créer).

Figure 198: Créer un détenteur

Inventaire

Pour utiliser l'inventaire, cliquez sur **Organize (Organiser)** > **Scopes and Inventory** (Portée et inventaire) dans la barre de navigation de gauche.

Recherche dans l'inventaire

Tout l'inventaire détecté sur le réseau peut faire l'objet d'une recherche. Pour rechercher dans l'inventaire, utilisez le bouton **Search Inventory** (rechercher dans l'inventaire). Chaque article de l'inventaire est identifiable de manière unique par son adresse IP et son Instance virtuelle de routage et de transmission (VRF) et peut être utilisé pour effectuer une recherche. Il n'est pas possible de rechercher un élément d'inventaire de service à l'aide de son adresse IP. Utilisez l'une des étiquettes d'utilisateur associées au service, par exemple user_orchestrator_system/service_name, pour rechercher un inventaire de service. Une fois qu'un hôte a été trouvé, vous pouvez afficher des informations détaillées le concernant sur la page de profil d'hôte.

Éléments constitutifs de l'inventaire

1. Portée racine
   - Racine de la hiérarchie de la portée sous un détenteur donné
   - Fournit une séparation logique pour les domaines d'adresse L3
2. Champ d'application
   - Conteneur d'inventaire défini par une requête dynamique
   - Foundation pour le modèle de politique hiérarchique
   - Point d'ancrage pour la configuration des politiques, RBAC et des filtres

3. Filtre
   - Conception flexible basée sur une requête d'inventaire dynamique
   - Point d'ancrage pour la définition des intents, des services fournis et la définition de la politique

Note Comprend toutes les adresses IP des partenaires et tout ce qui communique dans votre environnement. Qu'ils soient accompagnés d'un agent ou non, vous devez définir ce qu'ils sont au moyen d'une étiquette.

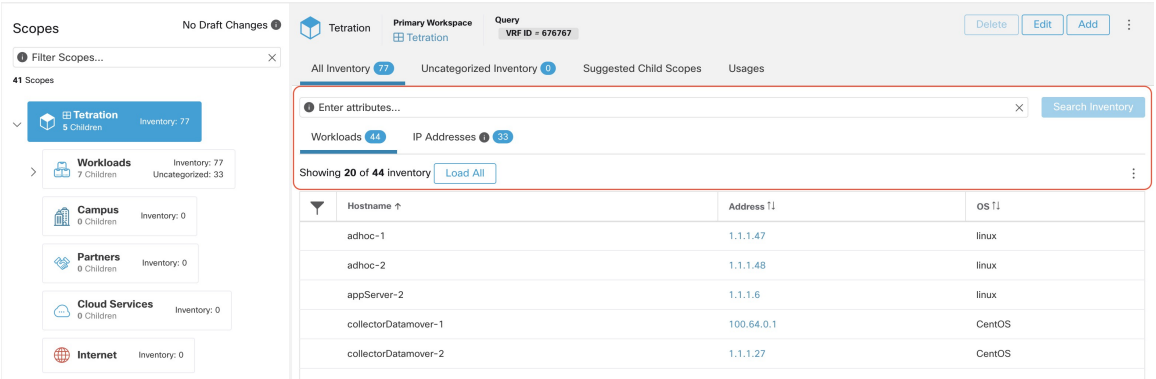
Facteurs à prendre en considération pour la planification des étiquettes

1. Source des données
   - Réseaux – IPAM? Tables de routage Feuilles de calcul?
   - Hôtes : CMDB, hyperviseur, nuage, propriétaires d'applications?
2. Exactitude des données
3. le niveau de dynamique des données et la façon dont elles seront mises à jour.
   - Chargement manuel?
   - Intégration d'API?
4. Commencez par les éléments de base et poursuivez la progression
   - Utilisez des étiquettes de réseau pour créer une structure de portée générale.
   - Utilisez des étiquettes d'hôte pour créer une structure de portée plus détaillée au niveau de l'application.

Rechercher dans l'inventaire

La recherche dans l'inventaire permet d'afficher des informations sur des éléments d'inventaire spécifiques.

Figure 199: Recherche dans l'inventaire



Procedure

Étape 1 Dans le volet de navigation, sélectionnez **Organize** > **Scopes and Inventory** (Organiser > Portées et inventaire).

Étape 2 Dans le champ **Filters** (Filtres), saisissez les attributs pour les éléments d'inventaire que vous recherchez. Les attributs sont les suivants :

Attributs	Description
Hostname (Nom d'hôte)	Saisissez un nom d'hôte complet ou partiel.
Nom VRF	Saisissez un nom de VRF
ID VRF	Saisissez un ID VRF (numérique).
Address (adresse)	Saisissez une adresse IP ou un sous-réseau valide (IPv4 ou IPv6).
Address Type (Type d'adresse)	Sélectionnez IPv4 ou IPv6.
SE	Saisissez un nom de système d'exploitation (p. ex., CentOS).
Version du système d'exploitation	Saisissez une version du système d'exploitation (p. ex., 6.5).
Interface Name (Nom d'interface)	Saisissez un nom d'interface (p. ex., eth0).
MAC	Saisissez l'adresse MAC.
Dans les règles de collecte?	Saisissez vrai ou faux.
Ligne de commande de processus	Saisissez la sous-chaîne d'une commande qui s'exécute sur l'hôte (Remarque : cet aspect ne peut pas être enregistré dans le cadre du filtre d'inventaire).
Traiter le condensé binaire	Saisissez le condensé de processus d'une commande qui s'exécute sur l'hôte (Remarque : cet aspect ne peut pas être enregistré dans le cadre du filtre d'inventaire).
Renseignements sur le paquet	Saisissez le nom du paquet, suivi facultativement d'une version du paquet (préfixée par #).
Paquet CVE	Saisissez une partie ou un ID CVE complet.
Note CVE v2	Saisissez une note CVSSv2 (Common Vulnerability Scoring System) (numérique
Note CVE v3	Saisissez une note CVSSv3 (Common Vulnerability Scoring System) (numérique).
Étiquettes d'utilisateur	Les attributs préfixés proviennent d'étiquettes d'utilisateur.

Étape 3 Cliquez sur **Search Inventory** (Rechercher dans l'inventaire). Les résultats sont affichés sous le champ **Filters** (filtres) regroupés dans quatre onglets. Chaque onglet comporte un tableau avec les colonnes pertinentes. Des colonnes supplémentaires peuvent être affichées en cliquant sur l'icône d'entonnoir dans l'en-tête du tableau. Si des étiquettes d'utilisateur sont disponibles, elles seront préfixées et peuvent être activées ici.

Figure 200: Résultats de la recherche d'inventaire

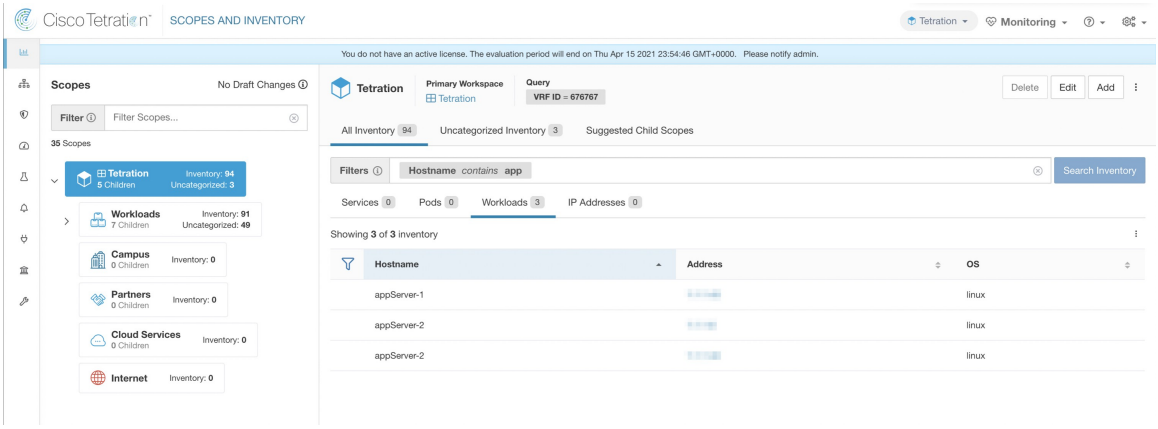
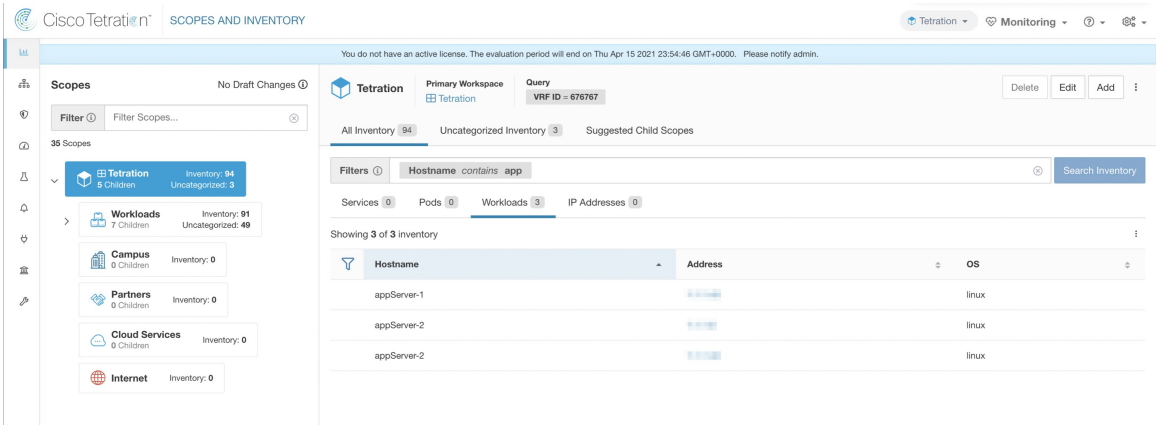


Figure 201: Résultats de la recherche d'inventaire



Les résultats de la recherche sont regroupés dans quatre onglets :

Onglet	Description
Services	Répertorie les services Kubernetes et les équilibreurs de charge détectés par les orchestrateurs externes. Cet onglet est masqué, sauf si un orchestrateur externe connexe est configuré.
Modules	Répertorie les pods Kubernetes. Cet onglet est masqué, sauf si un orchestrateur externe connexe est configuré.
Charges de travail	Répertorie les articles d'inventaire signalés par les agents Cisco Secure Workload.

Onglet	Description
Adresses IP	Répertorie les éléments de l'inventaire découverts par : • Téléversement de l'inventaire • Apprentissage des flux • Étiquettes téléversées manuellement • Étiquettes intégrées par les connecteurs et des orchestrateurs externes De plus, les listes de sous-réseaux signalés provenant des mêmes sources.

Note Par défaut, l'interception de tous les sous-réseaux pour les adresses IPv4 et IPv6 s'affiche dans chaque client hébergé.

Il y a également une mention du nombre d'inventaires à côté de chaque onglet. Les informations immédiatement disponibles lors d'hune recherche comprennent le nom d'hôte, les adresses IP avec les sous-réseaux, le système d'exploitation, la version du système d'exploitation, le nom du service et le nom du pod. La liste des colonnes affichées peut être modifiée en cliquant sur l'icône d'entonnoir dans l'en-tête du tableau. Les résultats de la recherche sont limités à la portée actuellement sélectionnée dans le répertoire des portées. Vous trouverez plus d'informations sur la page de profil respective en cliquant sur un élément dans les résultats de recherche.

Plus de détails sur chaque hôte sont affichés dans le **Profil de charge de travail**, accessible en cliquant dans le champ d'adresse IP d'une rangée de résultats de recherche. Consultez le Profil de la charge de travail pour en savoir plus.

Pour créer des filtres d'inventaire à l'aide de la barre latérale : Choisissez **Organize (Organiser)** > **Inventory filters (Filtres d'inventaire)** dans le menu supérieur. Cliquez sur le bouton **Create Filter** (créer un filtre). Une boîte de dialogue modale apparaît dans laquelle vous pouvez nommer votre filtre enregistré.

Suggérer des portées enfants

Suggest Child Scopes (Suggérer des portées enfants) est un outil qui utilise des algorithmes d'apprentissage automatique (comme la détection de communauté dans les réseaux) pour découvrir des groupes qui pourraient servir de portées . Cet outil est utile lors de la création d'une hiérarchie de portées et facilite le processus de définition de portées enfants plus granulaires pour une portée donnée. Les portées enfants candidates sont affichées sous forme de suggestions, qui peuvent ensuite être sélectionnés et ajoutés.

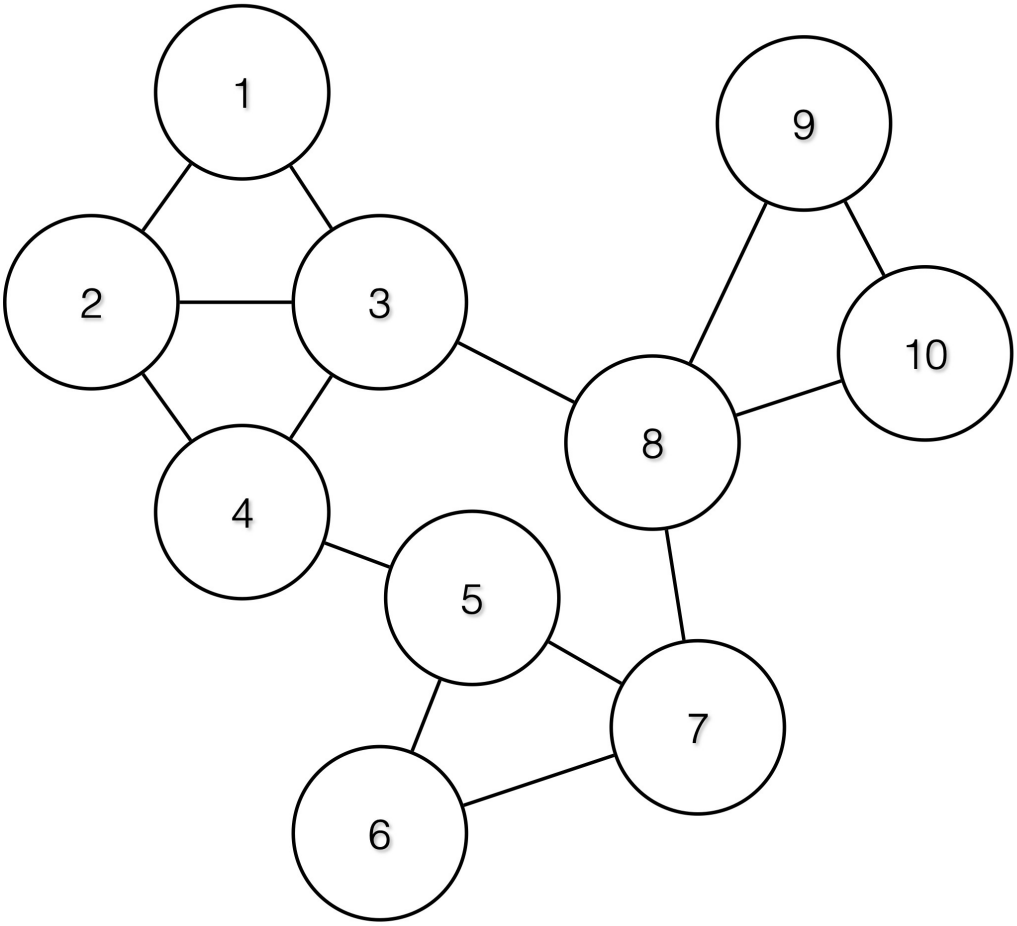
Description des algorithmes : Un graphe basé sur les communications entre les membres non réclamés de la portée parentale est d'abord créé (note : les membres non réclamés sont ceux qui n'appartiennent à aucune portée enfant de la portée parentale), et le graphe est prétraité, par exemple les algorithmes tentent d'identifier les points terminaux qui communiquent avec une proportion suffisamment élevée d'autres points terminaux dans le graphe. Un tel groupe de points terminaux, le cas échéant, est affiché pour l'utilisateur en tant que groupe candidat **de services communs**. Le reste du graphique est traité pour détecter les groupes qui se comportent comme **des communautés**, ce qui signifie en gros que les points terminaux communiquent entre eux de manière disproportionnée, plus souvent (ou sur plus de ports de fournisseur) qu'avec des points terminaux à l'extérieur du groupe. Chacun de ces regroupements peut correspondre à une application ou à un

service de l'l'entreprise. Un tel découpage peut également conduire à des politiques plus éparses entre les portées.

Exemple :

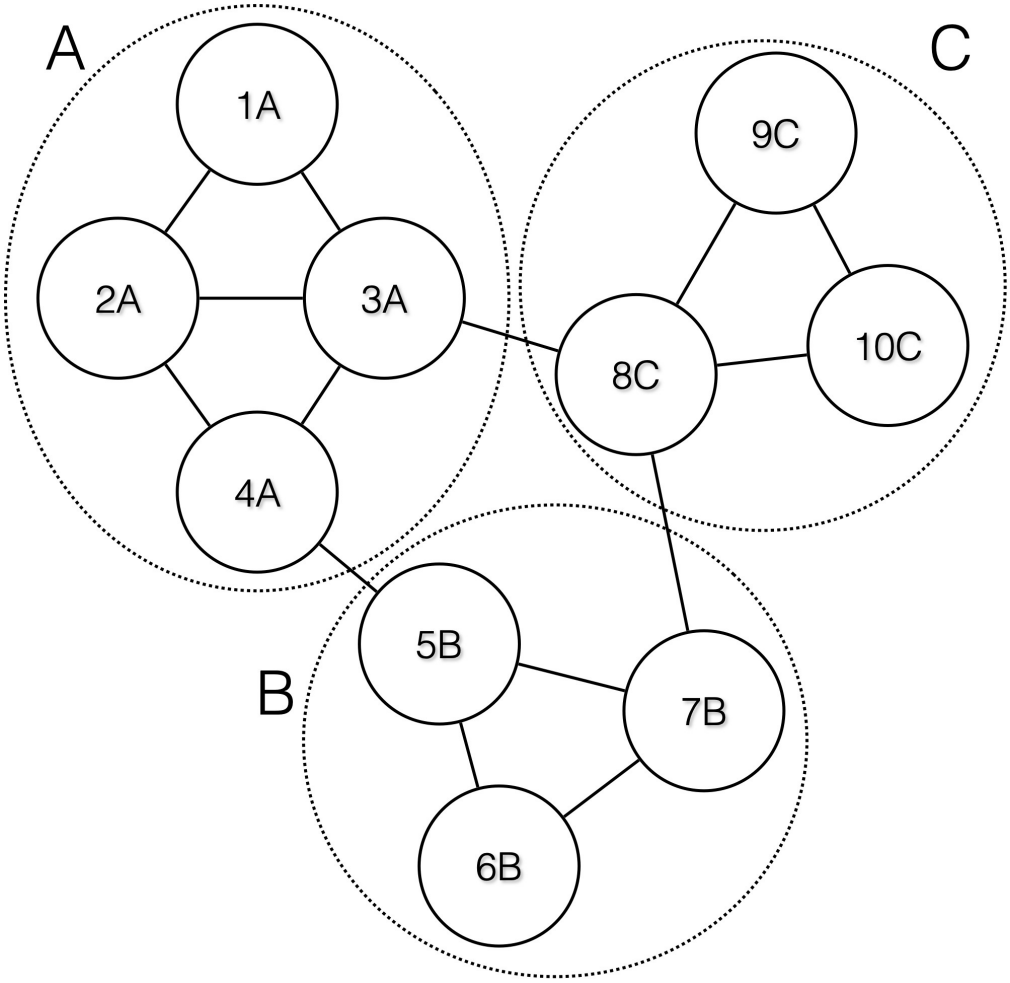
Les chiffres 1 à 10 représentent les adresses IP individuelles des points terminaux. Supposons que le graphique d'entrée (des communications) soit le suivant :

Figure 202: Graphique d'entrée



Ainsi, les points terminaux 1 à 4, 5 à 7 et 8 à 10 seront regroupés, car ils ont un degré de communication relativement élevé (nombre de périphéries) entre eux et de relativement faibles communications avec d'autres points terminaux.

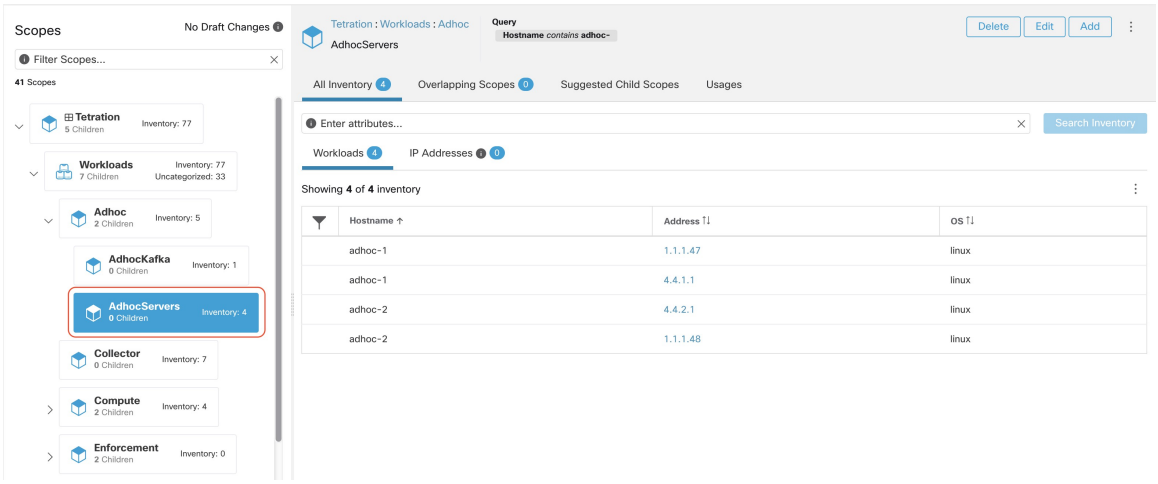
Figure 203: Groupes de sortie



Étapes de la proposition de portées

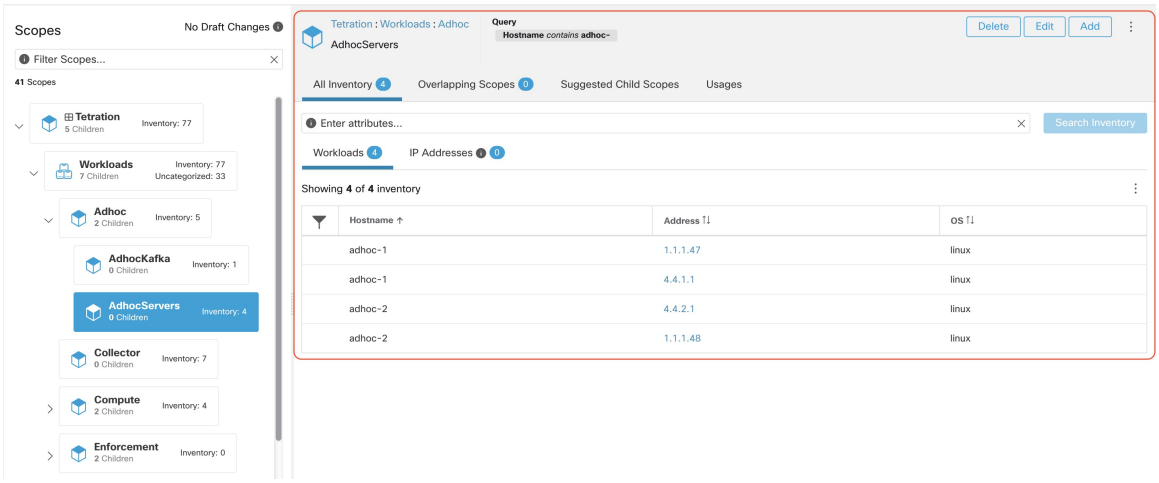
Pour invoquer la suggestion de portée pour une portée souhaitée, l'utilisateur doit se rendre sur la page des portées et la sélectionner.

Figure 204: Sélectionner une portée



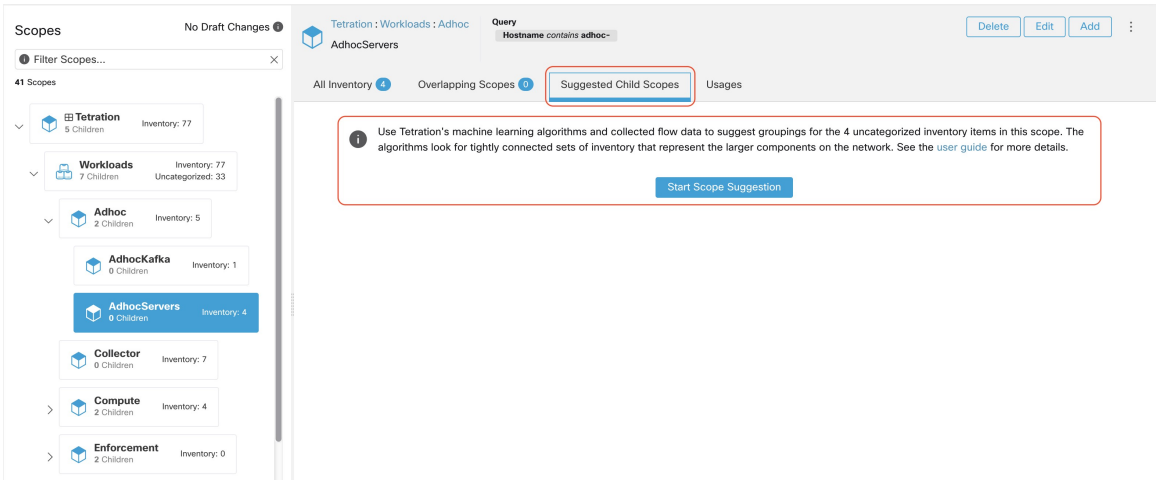
Dans la fenêtre, l'utilisateur peut parcourir l'inventaire, les *articles stockés non classés*, c'est-à-dire les articles qui appartiennent à la portée actuellement sélectionnée et qui n'appartiennent à aucune des portées enfants de la portée actuellement sélectionnée. Cliquer sur les **uncategorized inventory items (articles d'inventaire non classés)** pour afficher cette liste.

Figure 205: Fenêtre de portée



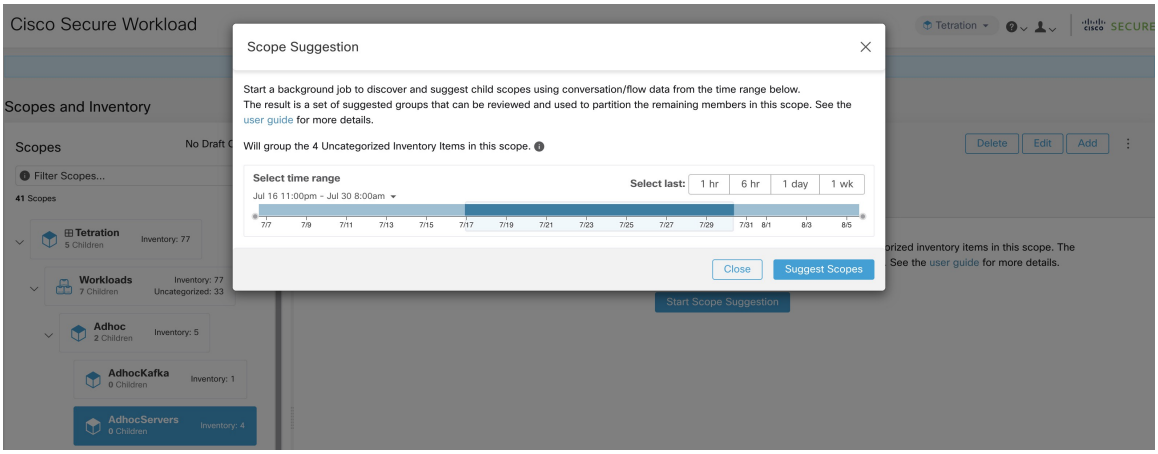
Après avoir sélectionné la portée, l'utilisateur peut cliquer sur **Suggest Children Scope** (Suggestions de portées enfants), puis sur **Start Scope Suggestion** (Démarrer la suggestion de portée) (ou cliquer sur Rerun, (Réexécution) si ce n'est pas la première fois). Notez que l'entrée d'un cycle de suggestion de portée sera les articles en inventaire non catégorisés.

Figure 206: Portées enfants



L'utilisateur peut définir la plage de dates comme entrée pour la suggestion de portée et cliquer sur **Suggest Scopes** (Suggérer des portées). L'exécution d'une suggestion de portée est souvent rapide lorsque la charge globale est moyenne, et ne prend que quelques minutes pour traiter des dizaines de milliers de points terminaux, comportant des dizaines de milliers de conversations.

Figure 207: Sélecteur de plages de données de suggestions de portée

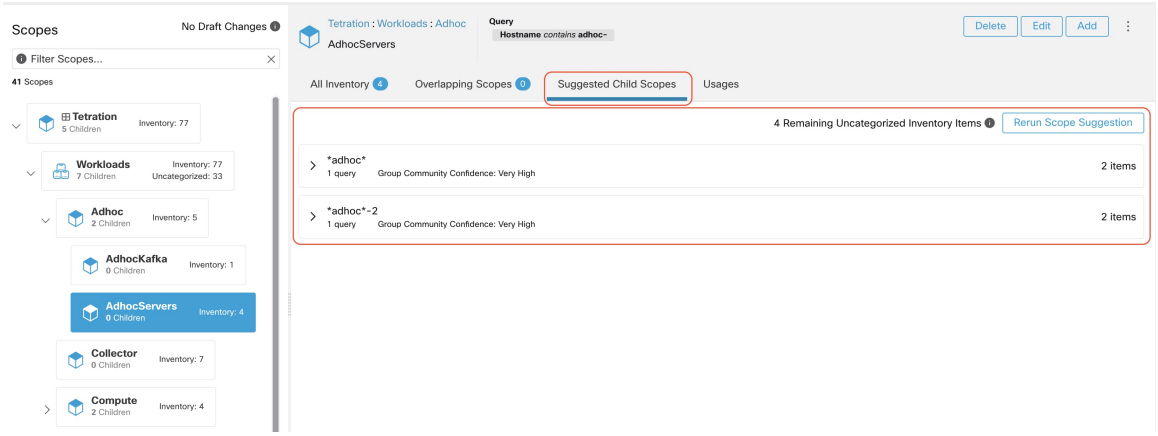


Le résultat est présenté à l'utilisateur sous la forme d'une liste de candidats, actuellement jusqu'à 20 groupes (illustrés), chacun accompagné d'informations telles que la confiance dans le groupe (qualité), le nom de la portée du candidat et les requêtes. Chaque groupe découvert est associé à un **niveau de confiance de la communauté de groupe**. Les valeurs possibles sont les suivantes : **très élevée**, **élevée**, **moyenne** et **faible**. Il s'agit d'une mesure de la propriété **communauté** du groupe : plus la confiance est élevée, plus la propriété communautaire du groupe donné de points terminaux est élevée (beaucoup de périphéries à l'intérieur du groupe, relativement peu de périphéries vers l'extérieur). Actuellement, le sous-ensemble de groupes à afficher sont sélectionnés en fonction de la confiance de la communauté du groupe. Les groupes découverts peuvent actuellement appartenir à l'un de ces quatre types de groupes :

- **Groupe générique** : tout groupe découvert par apprentissage automatique en fonction de la propriété de la communauté. Notez que tout groupe qui n'est pas explicitement désigné avec les types spéciaux ci-dessous est un groupe générique.

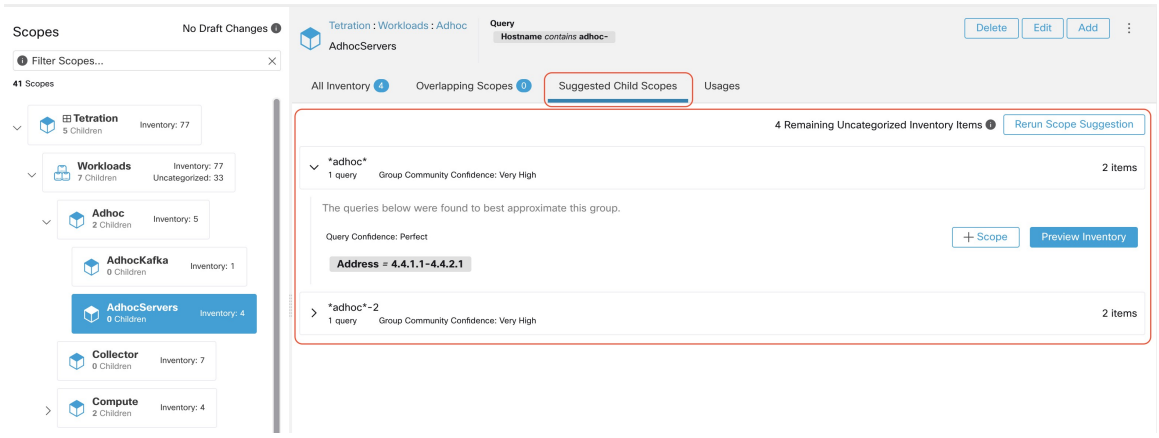
- **Services communs** : ce groupe se compose de terminaux qui communiquent avec une grande partie de l'inventaire d'entrée. Ces points terminaux exécutent peut-être des services partagés.
- **Clients des services communs** : ce groupe se compose de points terminaux qui communiquent uniquement avec le groupe **de services communs**.
- **Non groupé** : ce groupe se compose de points terminaux qui ne peuvent pas être regroupés, car leurs communications ne sont pas suffisantes.

Figure 208: Sortie des suggestions de portée



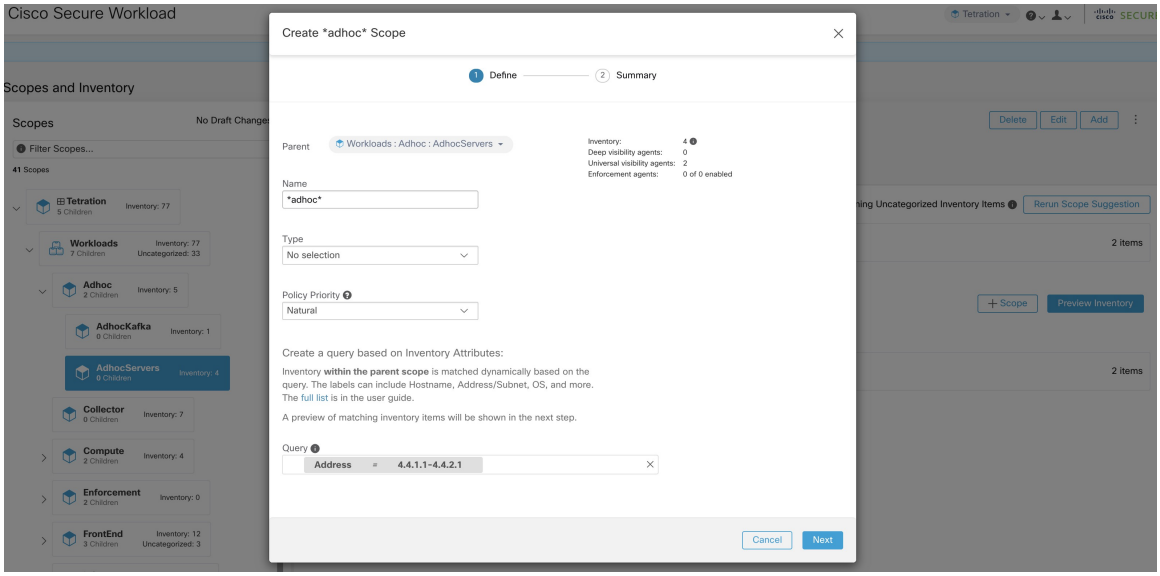
L'utilisateur peut cliquer sur un groupe découvert pour afficher la liste des requêtes générées pour le groupe sélectionné. L'utilisateur peut avoir un aperçu de l'inventaire couvert par la requête, qui définira avec précision le groupe découvert. Les requêtes consistent en des plages d'adresses IP, des sous-réseaux, des noms d'hôte et des étiquettes téléversées par l'utilisateur. Une mesure de confiance est associée à chaque groupe appelé **Query confidence** (confiance de la requête) qui peut avoir l'une des plages de valeurs suivantes : **Idéale**, **très élevée**, **élevée**, **moyenne** et **faible**. Pour la génération de requêtes, les groupes sont d'abord détectés par traitement de graphique et apprentissage automatique, puis les requêtes sont générées pour chaque groupe. Le niveau de **confiance de la requête** est une mesure de la capacité de la requête à couvrir les points terminaux. Un niveau de confiance de requête **Perfect** (idéal) indique que la requête couvre exactement le groupe suggéré (découvert). À l'autre extrême, un niveau de confiance de requête **Low** (faible) indique que la requête manque de manière significative la capture exacte du groupe suggéré, ce qui signifie que la requête couvre de nombreuses **adresses IP supplémentaires** (ne faisant pas partie du groupe découvert) et/ou a de nombreuses **adresses IP manquantes** (non couvertes par la requête).

Figure 209: Requêtes de sortie des suggestions de portée



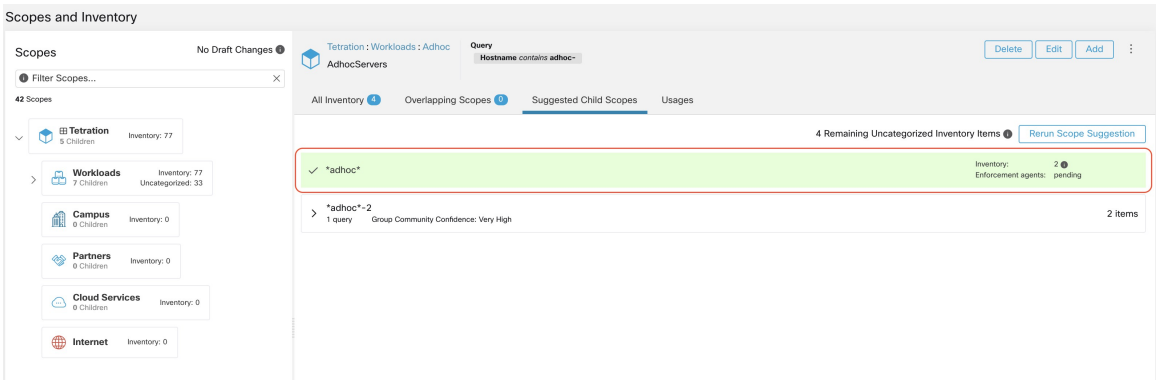
L'utilisateur peut cliquer sur le bouton **+ Scope** (+ Portée), ce qui le mènera à une fenêtre de modification dans laquelle il pourra modifier le nom du groupe et la requête de groupe. L'utilisateur peut examiner une requête, les adresses IP auxquelles elle correspond et décider si certaines adresses IP doivent être ajoutées ou supprimées en ajustant la requête. Une fois satisfait, l'utilisateur peut cliquer sur **Next**(suivant) pour examiner et convertir le groupe en une portée sur le sur le canevas de la vue préliminaire.

Figure 210: Fenêtre de modification des suggestions de portée



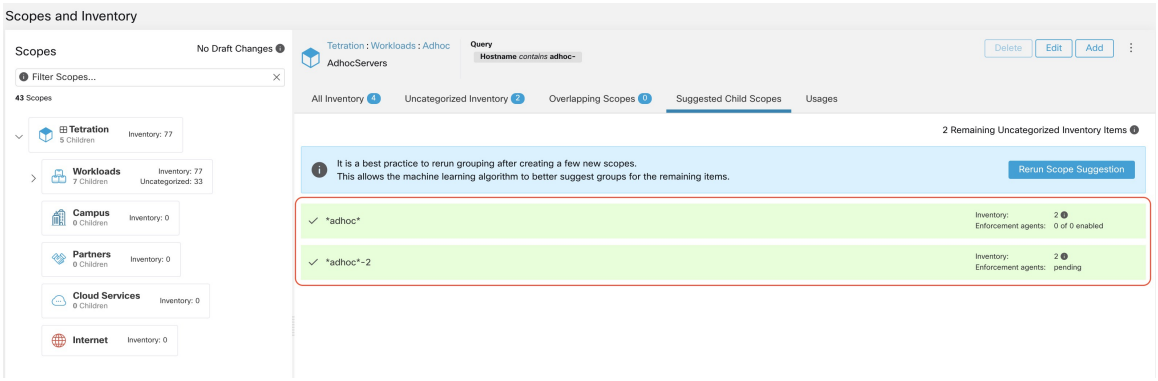
Une fois que l'utilisateur a converti un groupe suggéré en portée, l'emplacement de groupe devient vert et le **nombre Uncategorized Inventory Items (d'éléments en stock non catégorisés)** diminue.

Figure 211: Exemple de résultat de suggestion de portée après conversion d'un groupe suggéré en portée



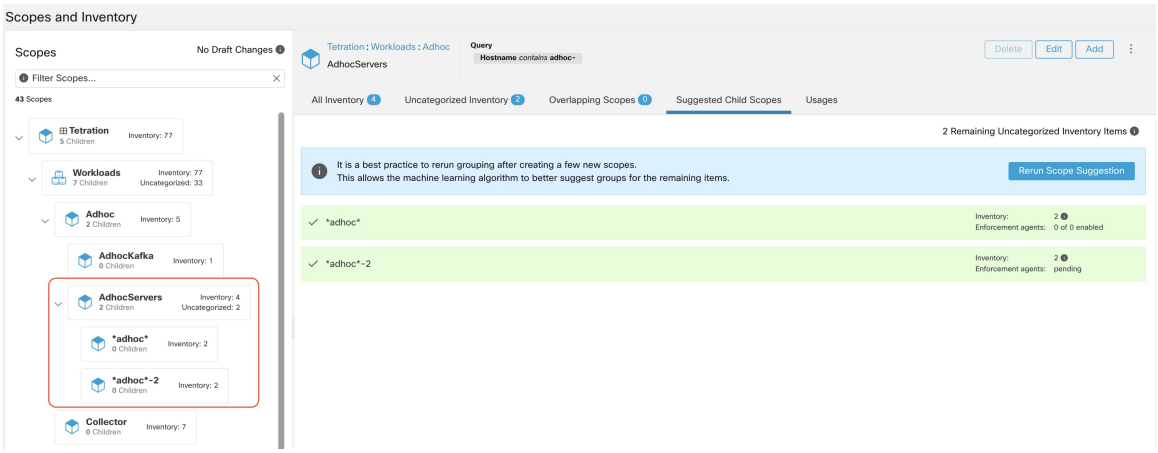
L'utilisateur peut répéter le processus de création de portée à partir de la liste de groupes restante. Le flux de travail recommandé est de créer une ou plusieurs portées, puis de réexécuter la **Suggestion de portée**. Un nombre nul **Uncategorized Inventory Items** (d'éléments d'inventaire non catégorisés) indique qu'il n'y a plus d'inventaire à délimiter (pour la portée parentale actuellement sélectionnée).

Figure 212: Résultat de suggestion de portée à partir de plusieurs créations de portée



Une fois le processus de création de portée terminé (le nombre non catégorisé est 0), l'utilisateur peut répéter ce processus sur les portées enfants nouvellement créées afin de générer une arborescence de portées plus approfondie, s'il le souhaite.

Figure 213: Liste des portées après la suggestion et la création de la portée initiale



Note Il est également possible que les éléments non catégorisés dans une portée ne se partitionnent pas bien (par exemple, qu'ils ne forment pas de communautés). Dans ce cas, l'algorithme peut ne renvoyer aucun regroupement (un résultat vide).

Filtres

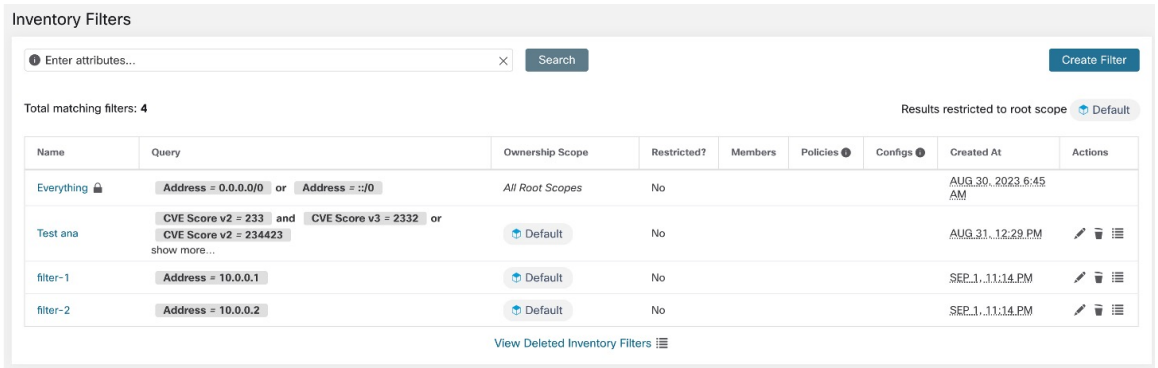
Les filtres sont des recherches d'inventaire enregistrées utilisées pour définir les politiques, les intents de configuration, etc. Évitez tout filtre associé à une portée, qui définit la portée de la propriété du filtre.

Pour afficher les filtres existants, cliquez sur **Organize (Organiser)** > **Inventory filters (Filtres d'inventaire)** dans la barre de navigation. Vous pouvez également afficher les filtres d'inventaire spécifiques à n'importe quel espace de travail pour n'importe quelle portée.

La liste des filtres est limitée en fonction de la racine de la portée actuellement sélectionnée.

Les filtres affichent également le nombre de membres, le nombre de politiques dans lesquelles il est impliqué, la somme des projets de politiques analysés et appliqués.

Figure 214: Filtres d'inventaire



Vous pouvez examiner les modifications apportées à l'appartenance à l'inventaire par rapport à la portée parente sélectionnée en consultant la fenêtre Examiner l'incidence des modifications de la portée/du filtre.

Créer un filtre d'inventaire

Créez des filtres d'inventaire pour :

- Créer ou découvrir des politiques spécifiques à des sous-ensembles de charges de travail dans une portée.

  Par exemple, créez un groupe de serveurs d'API dans la portée, les serveurs doivent être accessibles via l'interface d'API. Créez des politiques pour autoriser uniquement le trafic autorisé, mais bloquez l'accès à toutes les autres charges de travail pour cette application.

- Créez des politiques pour les charges de travail qui existent dans de nombreuses portées.

  Par exemple, pour créer une politique qui s'applique à toutes les charges de travail sur le réseau exécutant un système d'exploitation particulier, créez un filtre d'inventaire qui s'étend sur plusieurs ou sur toutes les portées.

Astuces Pour convertir une grappe existante en filtre d'inventaire, consultez Convertir une grappe en filtre d'inventaire, à la page 510.

Procédure

Étape 1 Accédez à l'un des emplacements suivants :

- Choisissez **Organize (Organiser) > Inventory filters (Filtres d'inventaire).**
- Accédez à n'importe quel espace de travail dans une portée pour lequel vous souhaitez créer un filtre d'inventaire et cliquez sur **Manage Policies** (Gérer des politiques) **> Filters** (Filtres).

Étape 2 Cliquez sur **Create Filter** (créer un filtre) ou **Add Inventory Filter**(ajouter un filtre d'inventaire).

Étape 3 Ajoutez un nom, une description et une requête qui inclut toutes les charges de travail, et seulement celles à inclure dans le filtre.

Étape 4 Cliquez sur **Show Advanced Options** (Afficher les options avancées).

Étape 5 Précisez la portée du filtre.

- Pour modifier le filtre, vous devez avoir un accès en écriture à la portée spécifiée ou à l'un de ses ascendants.
- (Selon les autres paramètres de cette procédure) Charges de travail incluses dans le filtre.

Étape 6 Configurer les options :

Destinataire	Faire ceci
Incluez les charges de travail qui répondent aux critères de requête du filtre, qu'elles soient ou non membres de la portée spécifiée dans ce filtre.	Désélectionnez **Restrict Query to Ownership Scope** (Restreindre la portée de la requête à la propriété)

Destinataire	Faire ceci
incluez uniquement les charges de travail qui sont membres de la portée spécifiée dans ce filtre.	Choisissez **Restrict Query to Ownership Scope** (Restreindre la requête à la portée de la propriété).
Autorisez la découverte automatique des politiques à suggérer des politiques spécifiques à l'ensemble de charges de travail défini par ce filtre. Ces charges de travail doivent constituer un sous-ensemble de la portée spécifiée dans le filtre.	Sélectionnez **Restrict Query to Ownership Scope (Restreindre la requête à la portée de la propriété)** et **Provides a Service External of its Scope (fournit un service externe à sa portée).** Pour utiliser ce filtre, vous devez configurer des dépendances externes. Pour en savoir plus, consultez Ajuster les dépendances externes d'un espace de travail, à la page 464.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Passez en revue les renseignements détaillés et cliquez sur **Create** (Créer).

Créer un filtre de domaine

Utilisez un filtre de domaine pour regrouper les domaines et identifier les flux pour lesquels un nom de domaine de consommateur ou de fournisseur correspond au filtre défini dans votre environnement.

En mode conversation, seuls certains types de serveurs mandataires sont pris en charge pour l'application du domaine, comme les mandataires HTTP et TCP. Dans le cas de TCP, lorsqu'un domaine est bloqué par un intent, le premier paquet peut le traverser; cependant, la connexion est bloquée avant même la fin de l'établissement de liaison.

Règles pour les filtres de domaine

- Vous ne pouvez saisir que deux noms de domaine dans le champ de **requête**, par exemple mail.cisco.com ou domain name=*cisco.com. Les noms de domaine tels que .com, .org ou .net ne sont pas pris en charge.
- Chaque étiquette du nom de domaine ne peut contenir que des lettres, des chiffres ou un tiret.
- Utilisez le caractère générique * dans le nom de domaine et uniquement pour la première étiquette, par exemple .Amazon.com, mais n'utilisez pas aws.com. De plus, ne combinez pas les caractères génériques avec d'autres caractères à l'aide de l'expression régulière, par exemple, n'utilisez pas aws*.com.
- Un caractère générique correspond à n'importe quel nombre d'étiquettes (sous-domaines), par exemple, .yahoo.com correspond à finance.yahoo.com, web.finance.yahoo.com et à tous ses sous-domaines. Cependant, il ne correspond pas à yahoo.com.
- Le préfixe www est traité comme un sous-domaine et n'est donc pas traité comme le domaine lui-même; par exemple, google.com et www.google.com sont des domaines distincts.
- Ne limitez pas la portée des filtres d'inventaire. Si un objet correspond au filtre, appliquez-le à l'ensemble du détenteur en saisissant DOMAIN.

Procédure

Étape 1 Accédez à l'un de ces emplacements :

- Choisissez **Organize (Organiser) > Inventory filters (Filtres d'inventaire).**
- Accédez à un espace de travail dans la portée pour créer un filtre d'inventaire, cliquez sur **Manage Policies (Gérer les politiques)** > **Filters(Filtres)** > **Inventory Filters (Filtres d'inventaire).**

Étape 2 Cliquez sur **Create Filter** ou **Add Inventory Filter** (Ajouter un filtre d'inventaire) pour afficher la page Inventory Filter (filtre d'inventaire).

Étape 3 Cochez la case. **Domain Filter** (Filtre de domaine).

Étape 4 Saisissez un nom et une requête pour le filtre de domaine, puis cliquez sur **Next**(suivant).

Étape 5 Passez en revue les détails et cliquez sur **Create** (créer) pour créer un filtre de domaine.

Pour chaque nouveau filtre d'inventaire, créez un nouveau type d'objet correspondant qui définit le type d'objets pour les correspondances de filtre. Les valeurs possibles sont les suivantes :

- **INVENTORY (INVENTAIRE)** comprend les charges de travail, les services, les pods et les adresses IP.
- **DOMAIN (DOMAINE)** fait référence aux domaines. Le nom de domaine est la seule option disponible pour la mise en correspondance des domaines; toutes les autres options correspondent uniquement au type **INVENTORY**.

Vous pouvez créer un filtre hétérogène en utilisant le nom de domaine et une autre option avec un opérateur **OU** , par exemple domain name= `*.google.com` OR hostname that contains `mach`. Cependant, il n'est pas possible d'utiliser **AND** pour combiner ces aspects à l'aide de l'opérateur **AND**, par exemple domain name=`*.Google.com` **AND** hostname that contains `mach`.

Limiter à la portée de la propriété

Cochez la case **Restrict to Ownership Scope?** (Restriction à la portée de la propriété?) pour déterminer si la portée a une incidence sur l'inventaire qui correspond au filtre. Par exemple, dans la structure suivante :

1. Détenteur avec requête

   ```
   VRF ID = 3
   ```

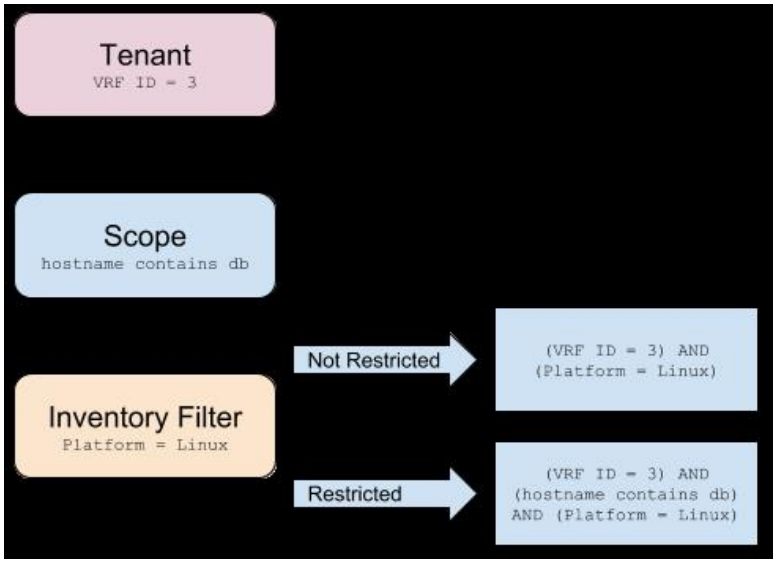
2. Portée au sein du détenteur avec la requête

   ```
   hostname contains db
   ```

3. Filtre d'inventaire avec la requête suivante associée à une portée.

   ```
   Platform = Linux
   ```

Figure 215: Structure de filtre des détenteurs, de la portée et de l'inventaire



- Si vous ne choisissez pas **Restrict to Ownership Scope**(Restreindre à la portée de la propriété), le filtre correspond à tous les hôtes du détenteur qui correspondent également au filtre. Saisissez la requête suivante :

  ```
  (VRF ID = 3) AND (Platform = Linux)
  ```

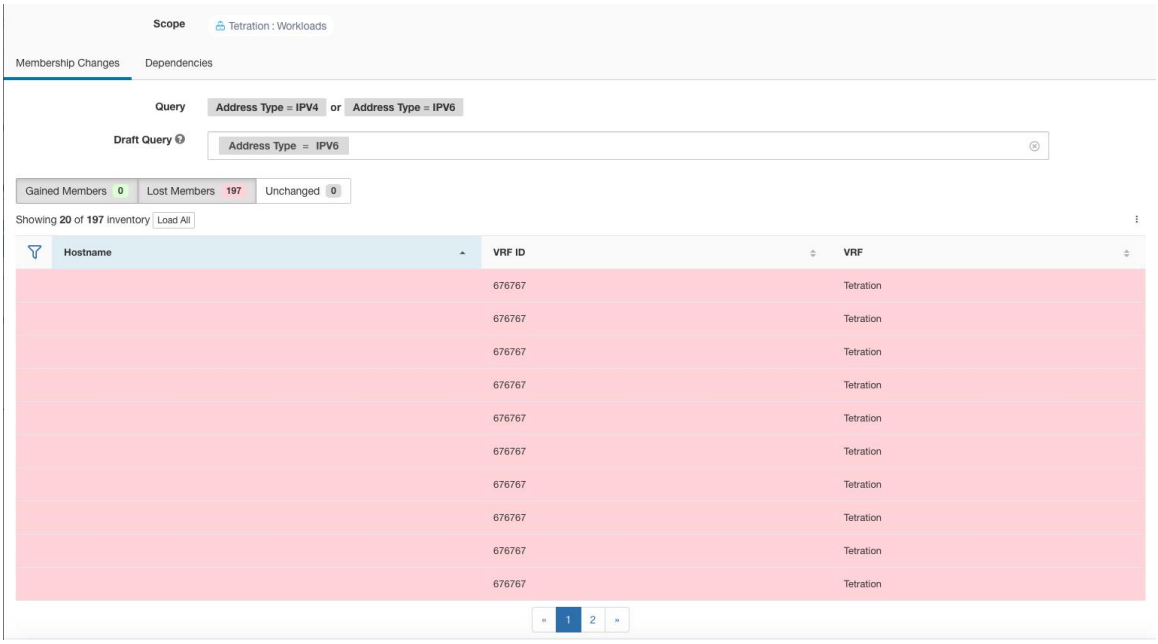
- Si vous choisissez **Restreindre à la portée de la propriété**, le filtre ne correspondra qu'aux hôtes du détenteur et de la portée qui correspondent également au filtre. Saisissez la requête suivante :

  ```
  (VRF ID = 3) AND (hostname contains db) AND (Platform = Linux)
  ```

Examiner l'incidence des modifications de la portée/du filtre

La mise à jour d'une requête de portée peut avoir une incidence sur les membres de l'inventaire de la portée après sa validation. De même, la modification de la requête de filtre, qui est enregistrée directement, peut également avoir une incidence sur les membres de l'inventaire de la portée. Vous pouvez identifier les changements de membres entre les nouvelles et les anciennes requêtes en suivant le lien **Review query change impact** (Examiner l'impact des modifications de requêtes) dans les boîtes de dialogue Scopes (Portée) ou Filter Edit (Modifier les filtres). En outre, connaître la portée ou les dépendances des filtres peut être utile pour l'analyse d'impact et la suppression de tous les objets nécessaires à la suppression de la portée. Visitez également l'onglet **Dépendances** pour parcourir l'arborescence des dépendances de la portée et obtenir de plus amples renseignements.

Figure 216: Télécharger le tableau des membres



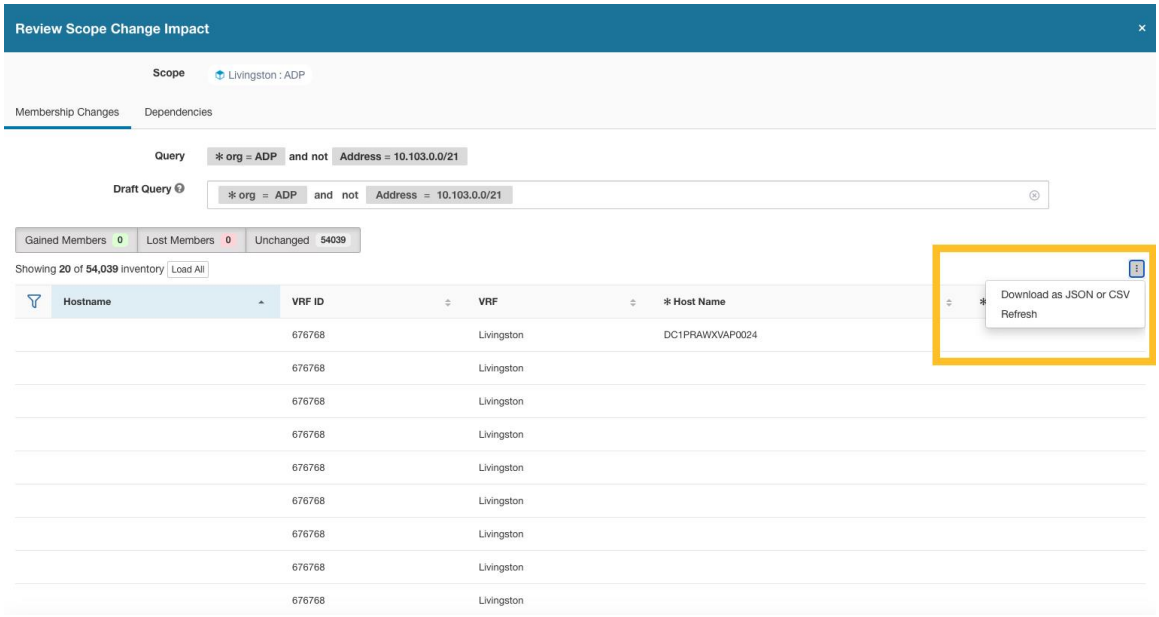
Boîte de dialogue de l'incidence de la modification de la requête de portée

Vous pouvez accéder à l'onglet **Membership Changes** (Modifications de l'adhésion) **Dependencies** (Dépendances) en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête) sur la fenêtre Scope Edit (Modification de la portée).

Modifications apportées aux membres

Le tableau d'inventaire sous la vue Membres affiche toutes les colonnes par défaut. Vous pouvez choisir les colonnes à afficher. En outre, vous pouvez télécharger le fichier csv ou json des colonnes et des lignes d'adhésion choisies avec une colonne Diff supplémentaire indiquant si l'inventaire est **gagné**, **perdu** ou **inchangé**. Assurez-vous que toute la sélection de tableaux que vous souhaitez télécharger est visible dans la vue du tableau.

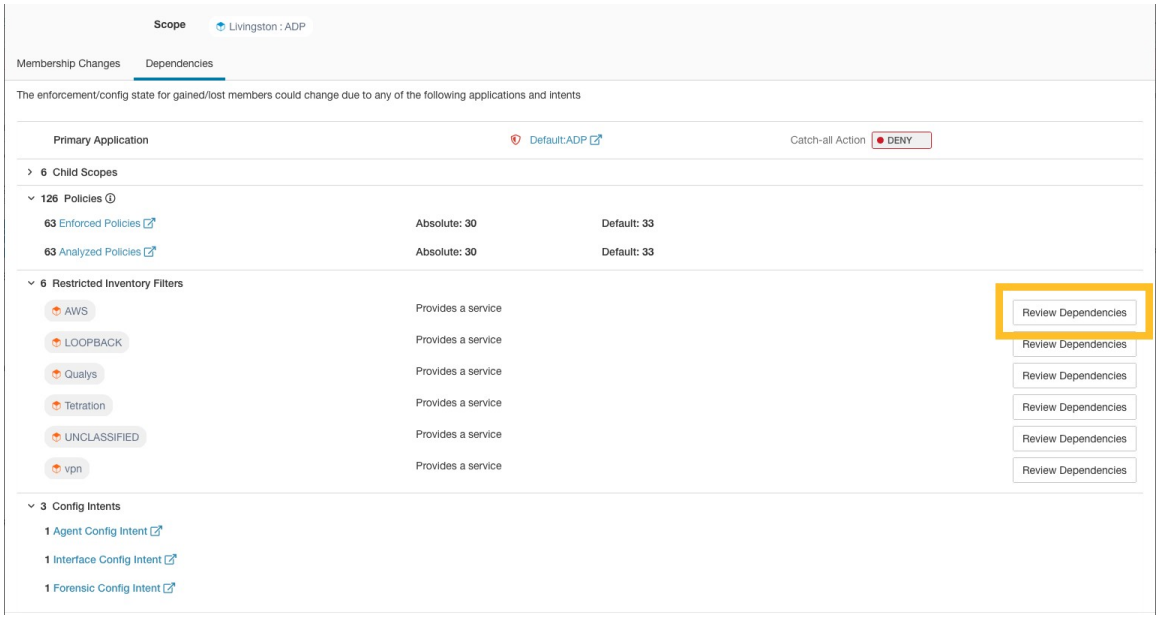
Figure 217: Modifications apportées aux membres de la portée



Dépendances

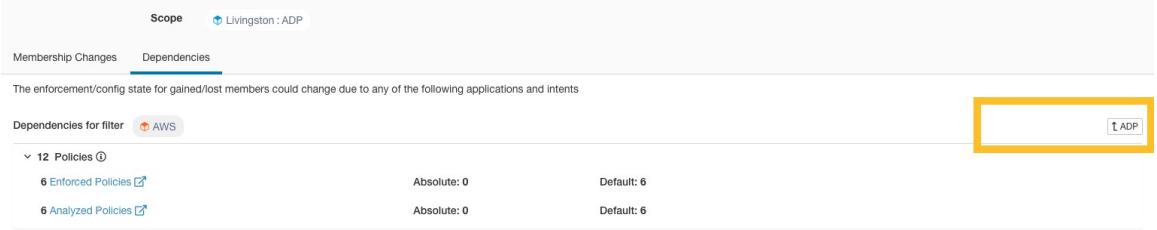
Vous pouvez parcourir les dépendances imbriquées en cliquant sur **Review Dependencies** (Examiner les dépendances).

Figure 218: Examiner les dépendances



Vous pouvez parcourir la sauvegarde de l'arborescence des dépendances en sélectionnant le lien parent sélectionné :

Figure 219: Lien parent



Les dépendances de portée qui peuvent exister sont les suivantes :

Table 22: Les dépendances de portée qui peuvent exister sont les suivantes

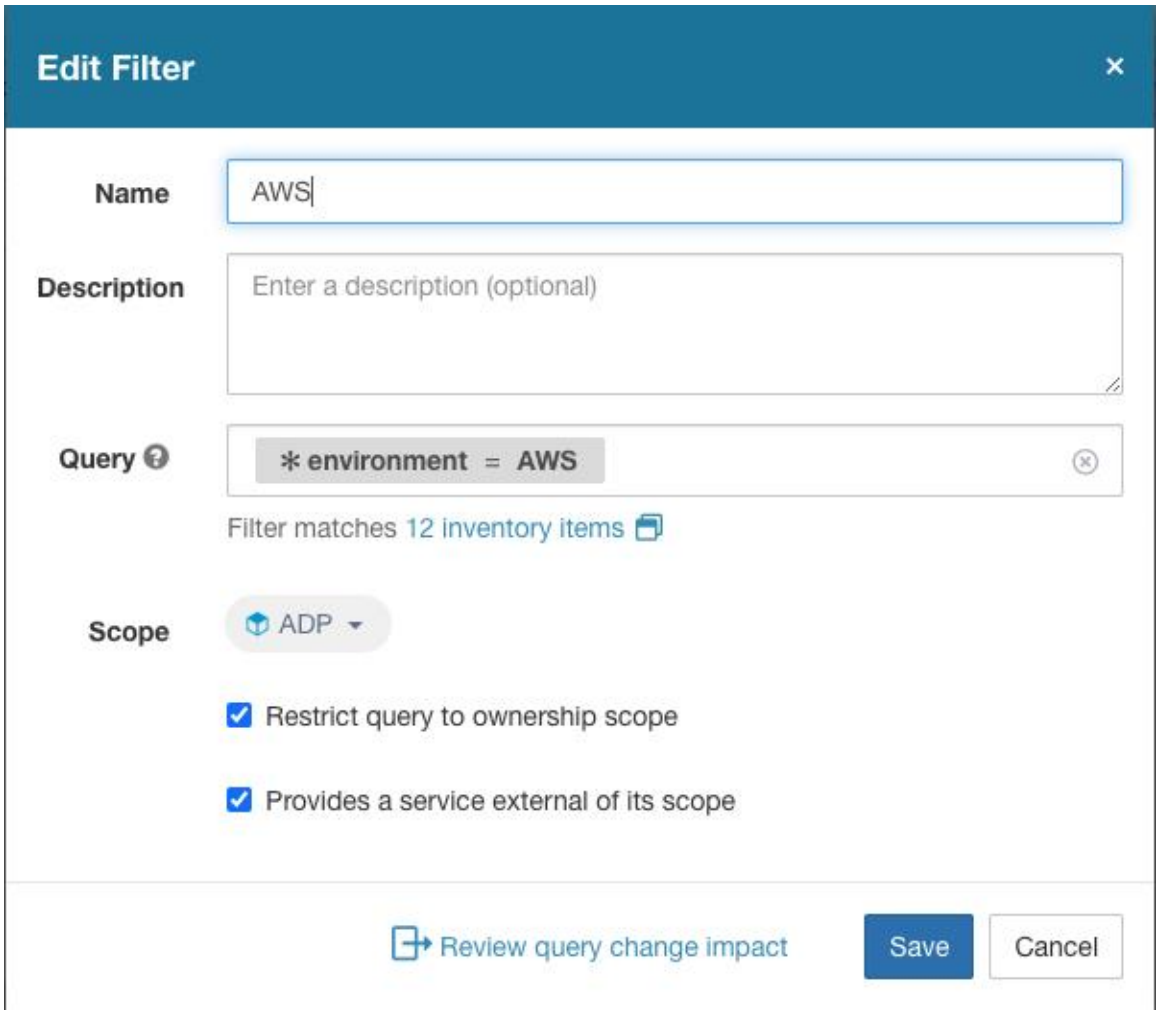
Type	Description
Application	Comporte des noms d'applications principales et secondaires et des liens vers des espaces de travail spécifiques dans la section Segmentation.
Portées enfants	Comporte des noms et des liens vers les vues détaillées de la portée enfant. Permet d'accéder aux dépendances de niveau inférieur.
Policies	A analysé et appliqué le nombre de politiques et les liens vers les vues de politiques globales respectives, filtrées par la portée sélectionnée.
Filtres d'inventaire restreint	Comporte des noms et des liens vers les vues détaillées des filtres enfants. Permet d'accéder aux dépendances de niveau inférieur.
Config Intents	Dispose de noms et de liens vers les affichages des intents de configuration d'agent, d'interface et criminalistiques.

Boîte de dialogue de l'incidence de la modification de la requête de filtre

Vous pouvez accéder à l'onglet **Membership Changes** (Modifications de l'adhésion) et à l'onglet **Dependencies** (Dépendances) en cliquant sur le lien **Review query change impact** (Examiner l'impact des modifications de la requête) dans la fenêtre de modification du filtre d'inventaire.

Modifications apportées aux membres

Figure 220: Modifications apportées aux membres pour le filtre d'inventaire



Dépendances

Voici les dépendances de filtres qui peuvent exister :

Type	Description
Policies	A analysé et appliqué le nombre de politiques et les liens vers les vues de politiques globales respectives, filtrées par la portée sélectionnée.
Config Intents	Dispose de noms et de liens vers les affichages des intents de configuration d'agent, d'interface et criminalistiques.

Profil d'inventaire

Note Il existe des liens vers une page de profil d'inventaire à partir de divers emplacements. L'une des façons d'afficher un profil d'inventaire consiste à effectuer une recherche d'inventaire, puis à cliquer sur une adresse IP pour accéder à son profil. Si vous travaillez dans la page Scopes and Inventory (Portées et inventaire), cliquez sur une adresse IP de l'onglet IP address (adresses IP), et non sur une adresse IP dans l'onglet Workloads (Charges de travail). (Cliquer sur une adresse IP dans l'onglet Workloads (Charges de travail) pour afficher le profil de charge de travail et non le profil d'inventaire).

Les renseignements suivants sont disponibles pour l'inventaire :

Champ	Description
Portées	Liste des portées à laquelle appartient l'inventaire.
Type d'inventaire	• L'inventaire **Flow learnt** (flux appris) a été enregistré en fonction des flux observés. • L'inventaire**Labeled** (étiqueté) a été téléversé manuellement à l'aide de l'utilitaire de téléchargement d'inventaire. • L'inventaire de l'**Agent** a été signalé par l'agent logiciel installé sur un hôte. • L'inventaire **Tagged** (marqué) a été signalé par les connecteurs ou par des orchestrateurs externes.
Étiquettes d'utilisateur	La liste des attributs téléversés par l'utilisateur pour cet inventaire. Consultez la section Étiquettes de charge de travail (Étiquettes d'utilisateur) pour en savoir plus.

Des renseignements supplémentaires ne sont disponibles que si les deux conditions suivantes sont remplies :

1. L'inventaire a été intégré par un connecteur infonuagique.
2. La segmentation est activée pour le réseau virtuel dans lequel se trouve l'inventaire.

Champ	Description
Intégrité de l'application	Les renseignements sur l'état de l'agent logiciel hôte. Consultez Onglet Agent Health (Intégrité de l'agent) (intégrité de l'agent) pour en savoir plus.

Champ	Description
Politiques concrètes	Cet onglet affiche politiques application concrètes de Cisco Secure Workload appliquées à l'hôte. Consultez Onglet Concrete Policies (Politiques concrètes) (Politiques concrètes) pour en savoir plus.
Groupes de sécurité	La liste des groupes de sécurité et leurs politiques appliquées à cet inventaire.

Renseignements sur le profil de l'inventaire

Champ	Description
Groupes **expérimentaux**	Une liste de filtres d'inventaire définis par la grappe ou par l'utilisateur qui sont utilisés pour l'analyse en temps réel des politiques.
Groupes d'**application**	Une liste des filtres d'inventaire définis par la grappe ou par l'utilisateur qui sont utilisés pour l'application des politiques. Ils peuvent être différents des groupes expérimentaux selon les versions des politiques analysées ou appliquées dans le système.

Note Les détails du profil d'inventaire peuvent ne pas être disponibles pour une adresse IP donnée dans les cas suivants :

- L'inventaire est exclu des règles de collecte.
- Dans un flux unidirectionnel, l'inventaire n'est disponible que pendant deux minutes, puis il est supprimé.
- Dans un flux bidirectionnel, l'inventaire est disponible pendant 30 jours. Si plus aucun flux n'est observé pendant ces 30 jours, les renseignements détaillés de l'inventaire sont supprimés.

Profil de la charge de travail

Le profil de charge de travail affiche des informations détaillées sur un hôte sur lequel un agent logiciel Cisco Secure Workload est installé. Cette section explique comment afficher un profil de charge de travail et les renseignements qu'il contient.

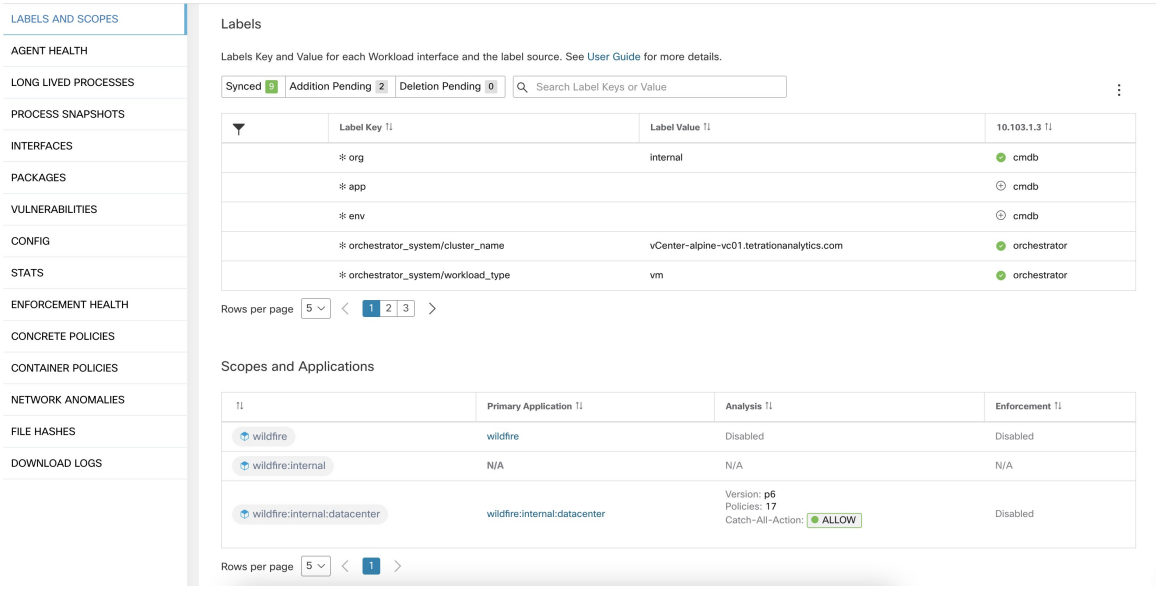
Note Il existe des liens vers une page de profil de charge de travail à partir de divers emplacements. L'une des façons d'afficher un profil de charge de travail consiste à rechercher un hôte comme décrit dans la section de recherche

Dans les résultats de la recherche d'inventaire, cliquez sur l'adresse IP de l'hôte pour accéder à son profil. En fonction du type d'agent installé sur l'hôte, les onglets suivants sont disponibles sur la page. Notez que vous pourriez vous aboutir à la page de profil d'inventaire si l'agent logiciel Cisco Secure Workload n'est pas installé sur l'hôte auquel cet inventaire appartient.

Onglet Labels and Scopes (Étiquettes et portées)

Cet onglet comprend les groupes d'applications et expérimentaux, auxquels l'hôte appartient. Les groupes expérimentaux sont des filtres d'inventaire utilisés pour l'analyse en direct des politiques, tandis que les groupes d'application sont des filtres utilisés pour l'application de celles-ci. Ils peuvent être différents selon les versions des politiques analysées ou appliquées dans le système.

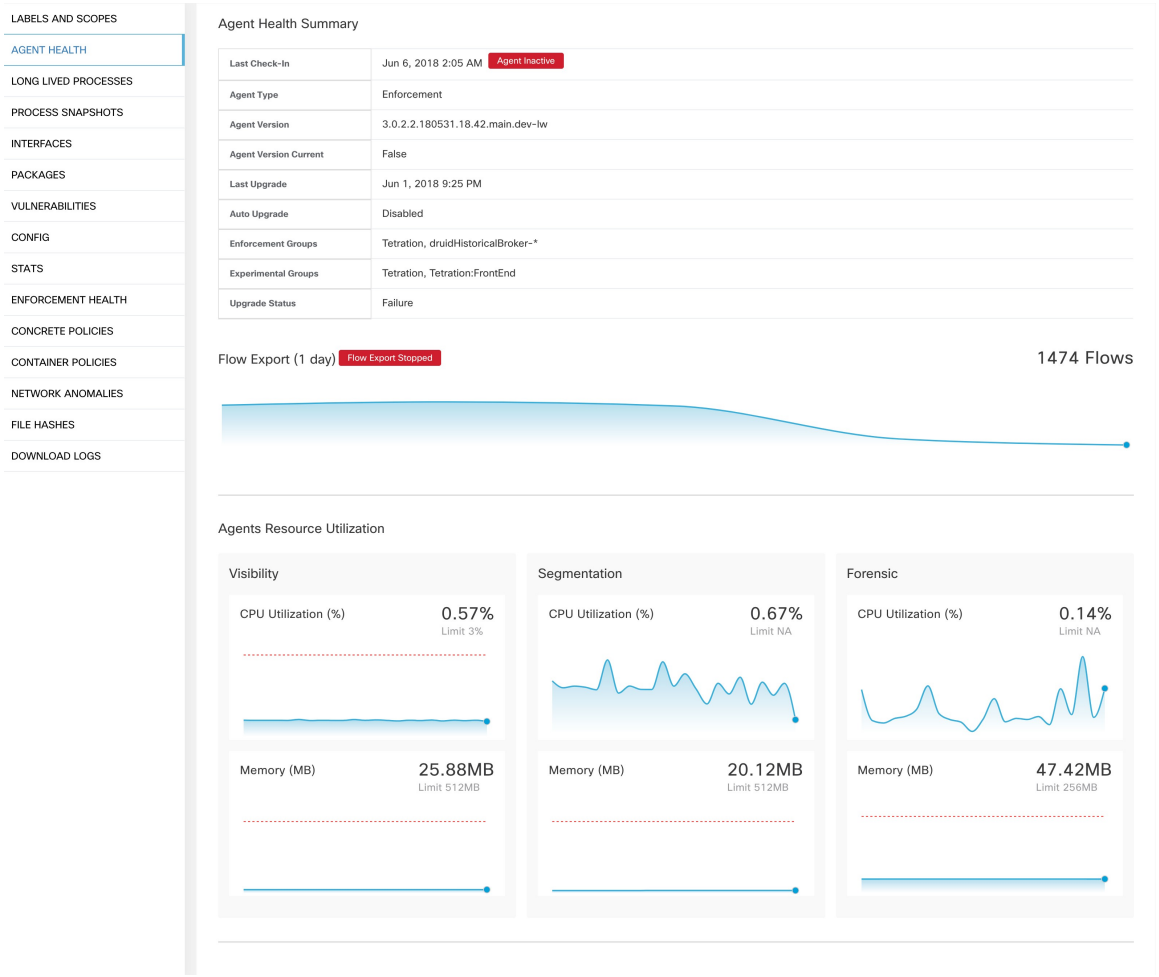
Figure 221: Étiquettes et portées de charge de travail



Onglet Agent Health (Intégrité de l'agent)

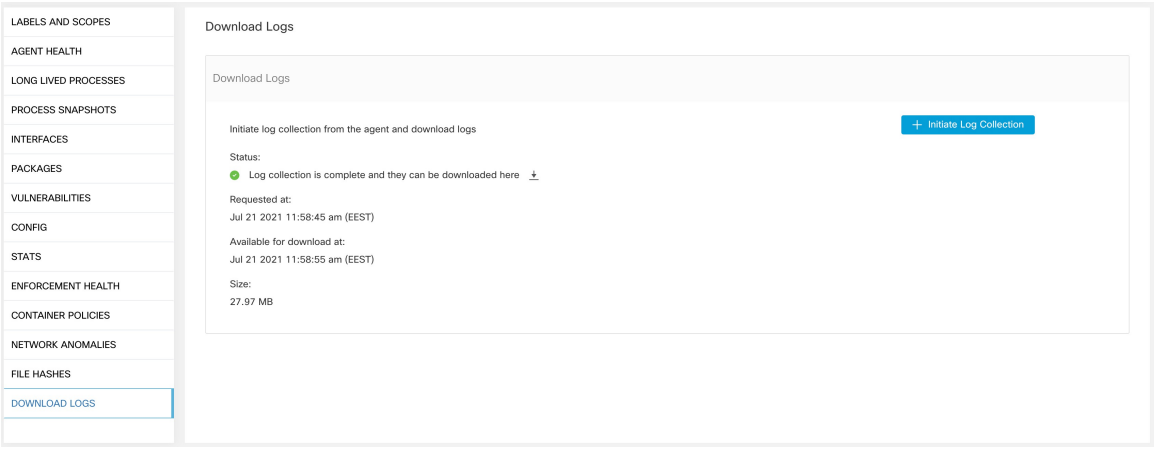
Les renseignements sur l'état de l'agent logiciel hôte, comme son type, la plateforme de système d'exploitation, la version de l'agent et l'heure de la dernière connexion, sont également affichés dans l'onglet **Agent Health (intégrité de l'agent)**. Reportez-vous à la section Configuration de l'agent logiciel pour en savoir plus. Cet onglet affiche également les données de série chronologiques détaillées pour les octets de trafic et les paquets générés pour une journée.

Figure 222: Détails de l'intégrité des agents de charge de travail



Pour les utilisateurs disposant de privilèges de propriétaire de portée racine, la page de résumé comprend également une section pour recueillir et télécharger les journaux des agents pour les agents de visibilité approfondie et d'application (versions 3.3 ou ultérieures) de cette portée racine. Notez également que cette fonction n'est pas disponible pour les agents exécutés sur les plateformes AIX et SUSE Linux Enterprise Server (s390x-Linux sur architectures IBM Z). Utilisez le bouton « Lancer la collecte des journaux » pour collecter les journaux de l'agent. Ces journaux sont disponibles pour téléchargement quelques minutes plus tard. Si le téléchargement échoue, réessayez de collecter les journaux, puis tentez à nouveau le téléchargement.

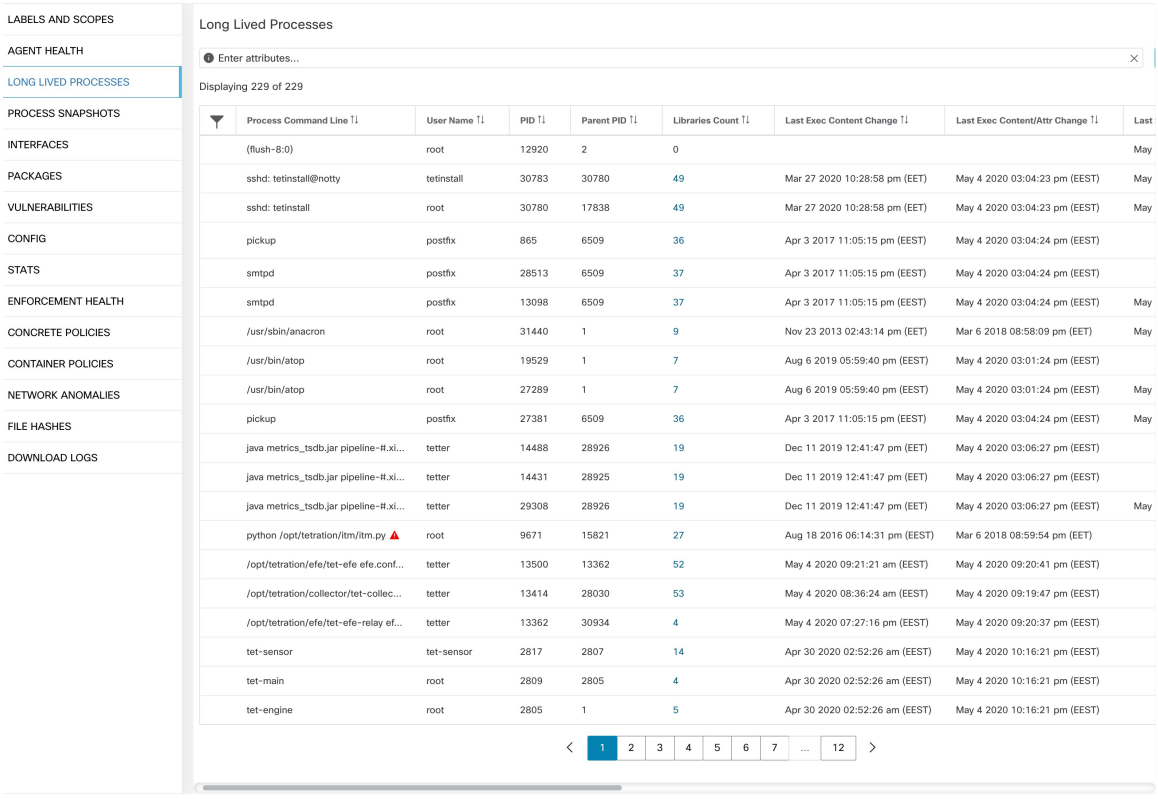
Figure 223: Journaux des agents



Onglet Liste de processus

Cet onglet affiche la liste des processus en cours d'exécution sur l'hôte. Un filtre est également disponible pour affiner la liste des processus en fonction des attributs d'un processus affichés dans l'en-tête du tableau ci-dessous.

Figure 224: Liste des processus de charge de travail



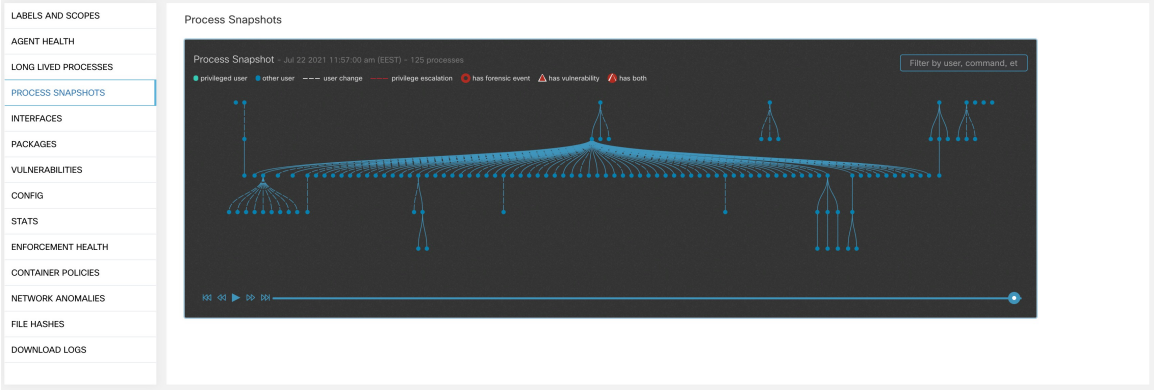
Descriptions des attributs :

Attribut	Description
Last Exec Content Change	Similaire à mtime dans Linux. Il s'agit de l'horodatage lorsque seul le contenu du fichier change.
Last Exec Content Change	Similaire à ctime dans Linux. Il s'agit de l'horodatage auquel le contenu ou l'attribut du fichier change.
Last Seen	Dernière fois que le processus est observé. Disponible lorsque le processus est arrêté.
Utilisation du processeur	Tendance d'utilisation du processeur par le processus au cours de la dernière heure.
Memory Usage	Tendance d'utilisation de la mémoire par le processus au cours de la dernière heure.
Traiter le condensé binaire	Condensé SHA256 du fichier binaire de processus dans la chaîne hexadécimale, également appelé condensé de processus. Non disponible pour les processus du noyau.
Note d'anomalie	Note de condensé de processus (anomalie). Consultez la section Process hash anomaly detection pour plus d'informations.
Verdict	Verdict du condensé du processus (soit malveillant, soit bénin). Le verdict est déterminé en fonction de l'appartenance du condensé du processus à une liste de condensés définie par l'utilisateur ou à une base de données de condensés connue de renseignements sur les menaces. Consultez la section Process hash anomaly detection pour plus d'informations.
Verdict Source	Source du verdict. La source de verdict peut être définie par l'utilisateur, Nuage Cisco Secure Workload ou NIST. Cet attribut est connu sous le nom de source de base de données de condensé dans les versions précédentes. Consultez la section Process hash anomaly detection pour plus d'informations.

Onglet Process Snapshot (Instantané du processus)

Cet onglet affiche l'arborescence des processus interrogeable observé pour la charge de travail.

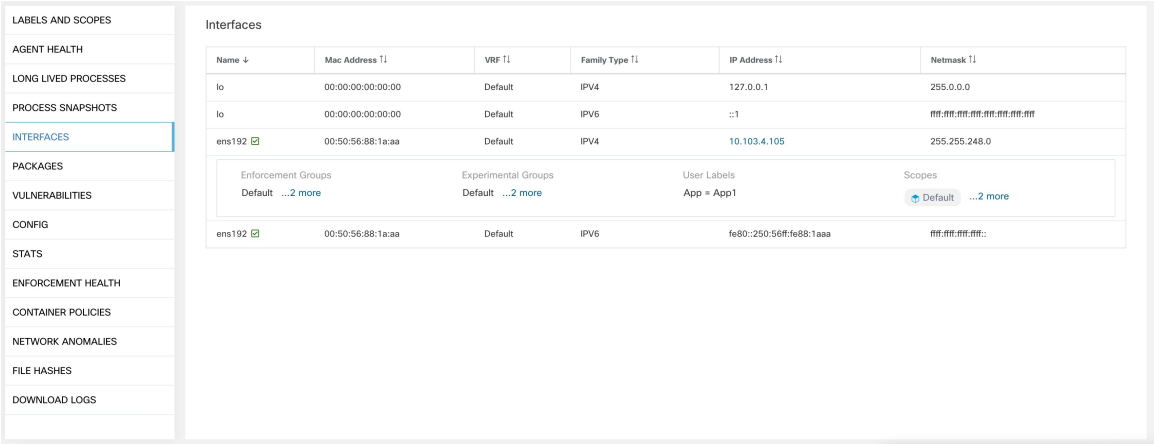
Figure 225: Instantané du processus de charge de travail



Onglet Interfaces

Cet onglet affiche des détails sur les interfaces réseau installées sur l'hôte. Il est disponible pour tous les types d'agents logiciels.

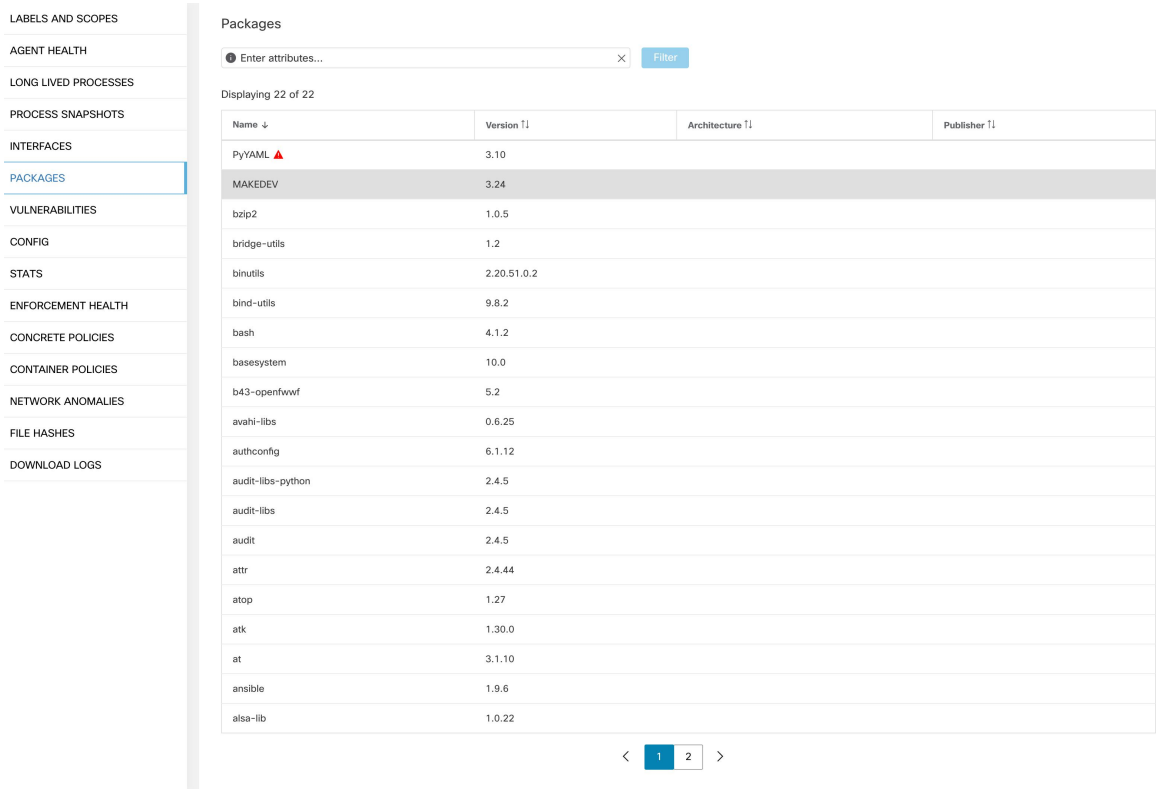
Figure 226: Liste des interfaces de charge de travail



Onglet Software Packages (Paquets logiciels)

Cet onglet affiche la liste des paquets logiciels installés sur l'hôte. Vous pouvez afficher de manière sélective les paquets logiciels en fonction des attributs du paquet dans l'en-tête du tableau.

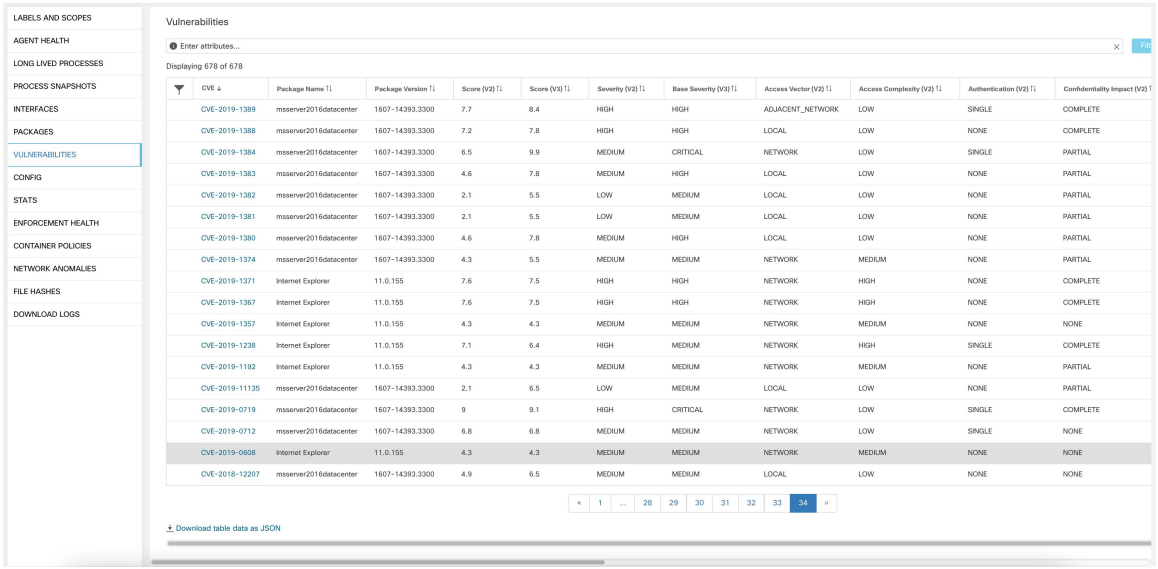
Figure 227: Liste des paquets logiciels



Onglet Vulnerabilities (Vulnérabilités)

Cet onglet affiche les vulnérabilités consultables observées sur la charge de travail en fonction des vulnérabilités et expositions courantes (CVE). Consultez la section Visibilité des données de vulnérabilité

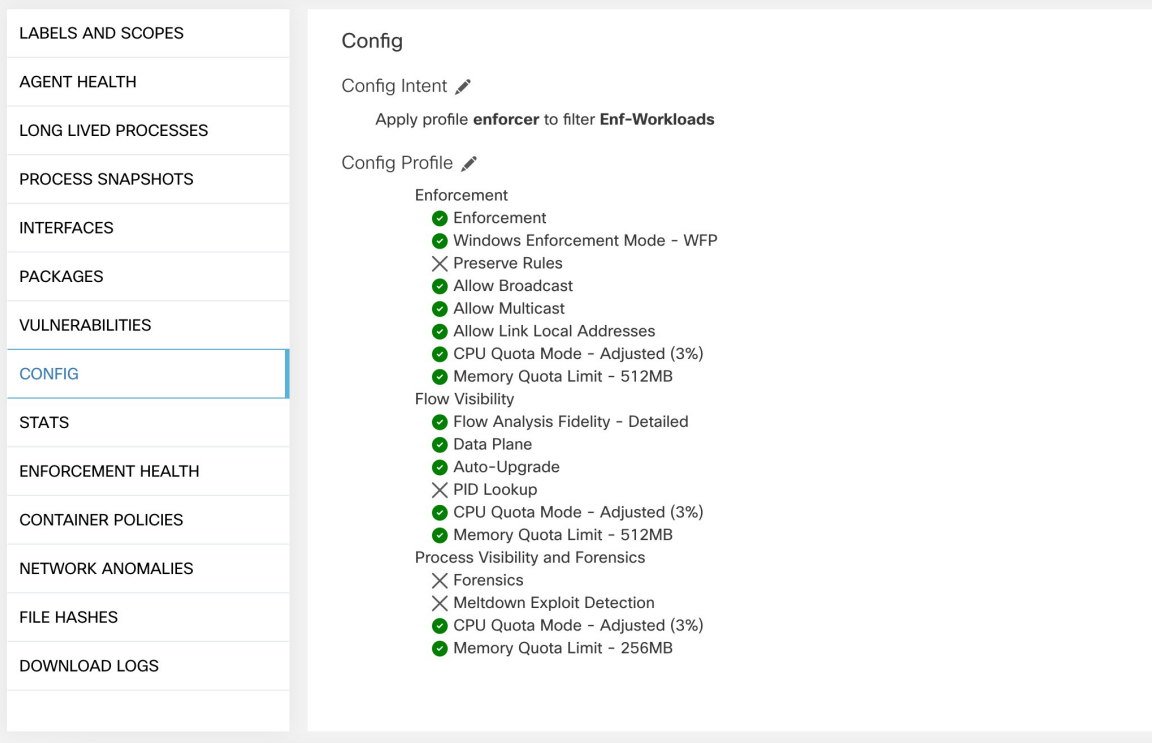
Figure 228: Onglet Vulnerabilities (Vulnérabilités)



Onglet Configuration de l'agent

Cet onglet affiche les paramètres de l’agent logiciel. Il est uniquement disponible pour les agents de visibilité approfondie et d’application. Ces paramètres peuvent être modifiés à l’aide des intents de configuration de l’agent via la page de configuration de l’agent. Voir Configuration de l’agent logiciel

Figure 229: Configuration de charge de travail appliquée



Onglet Statistiques de l'agent

Cet onglet affiche les statistiques sur l'agent Cisco Secure Workload installé sur l'hôte. Il est uniquement disponible pour les agents de visibilité approfondie et d'application.

Figure 230: Statistiques des agents

Onglet Concrete Policies (Politiques concrètes)

Lorsqu'un espace de travail est mis en œuvre, chaque charge de travail reçoit uniquement les politiques de cet espace de travail qui sont spécifiques à cette charge de travail. Ces politiques qui sont effectivement programmées sur chaque charge de travail sont appelées *politiques concrètes*.

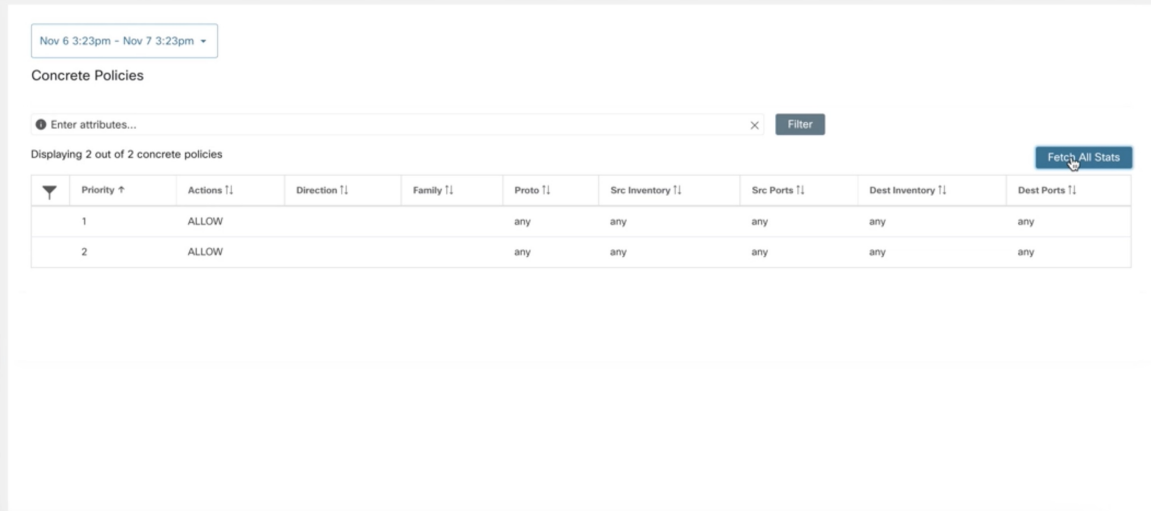
Par exemple, supposons que le fournisseur spécifié dans une politique avec l'action ALLOW (AUTORISER) inclue tout l'inventaire du sous-réseau 1.1.1.0/24. Lorsque cette politique est installée sur une charge de travail avec un agent Cisco Secure Workload et ayant l'adresse IP 1.1.1.2, les règles du pare-feu se présentent comme suit :

1. En ce qui concerne le trafic entrant, les règles du pare-feu autorisent le trafic destiné à l'adresse IP 1.1.1.2 en particulier, et non à l'ensemble du sous-réseau 1.1.1.0/24.
2. Pour le trafic sortant, les règles de pare-feu autorisent le trafic provenant dans la version 1.1.1.2 en particulier, et non de l'ensemble du sous-réseau 1.1.1.0/24.

L'onglet CONCRETE POLICIES (POLITIQUES CONCRÈTES) du profil de charge de travail affiche les politiques d'application concrètes de Cisco Secure Workload appliquées sur l'hôte. Chaque ligne de ce tableau correspond à une règle de pare-feu mise en œuvre sur l'hôte. Chaque ligne de politique peut être développée pour afficher l'intent logique dont cette politique concrète est dérivée. L'affichage de la série chronologique du nombre de paquets et d'octets est également disponible pour chaque règle. Cliquez sur le bouton **Fetch All Stats** (Récupérer toutes les statistiques) pour afficher le nombre de paquets et d'octets pour chaque règle. Un filtre est également disponible dans cet onglet pour réduire la liste des politiques appliquées en fonction

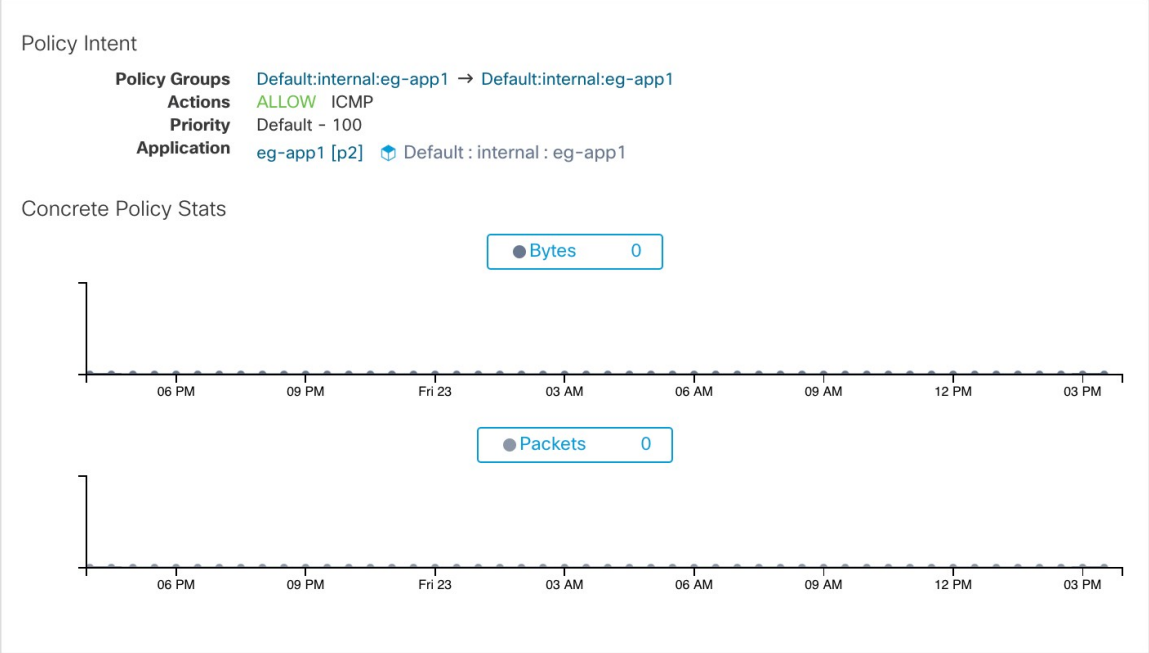
des attributs d'une politique indiqués dans l'en-tête du tableau ci-dessous. Cet onglet est disponible uniquement lorsque l'agent installé est activé pour la mise en application.

Figure 231: Liste de politiques concrètes



Dans l'image ci-dessous, les **groupes de politiques** affichent le consommateur et le fournisseur :

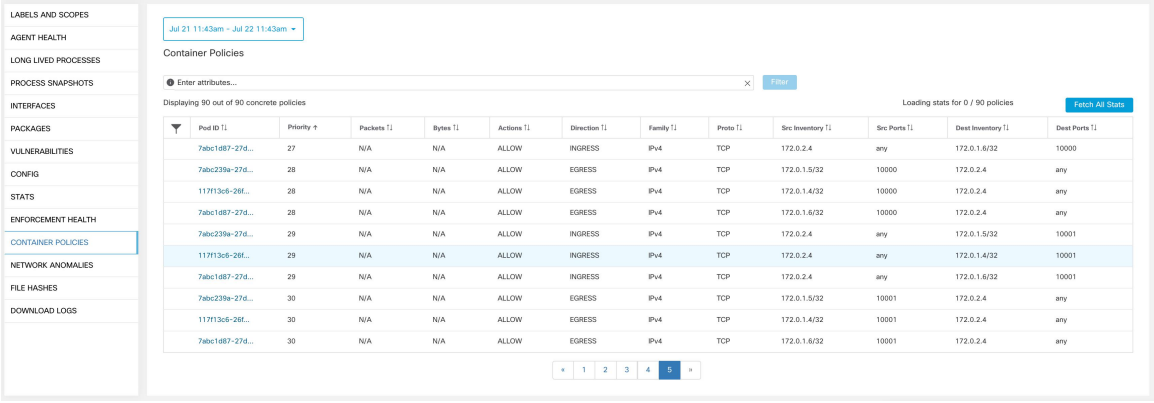
Figure 232: Ligne de politique concrète



Onglet Politiques de conteneur

Cet onglet affiche les politiques d'application concrètes Cisco Secure Workload appliquées aux conteneurs. Chaque ligne de ce tableau correspond à une règle de pare-feu mise en œuvre sur le pod de conteneur.

Figure 233: Liste des politiques concrètes de conteneur



Onglet Network Anomalies (Anomalie de réseau)

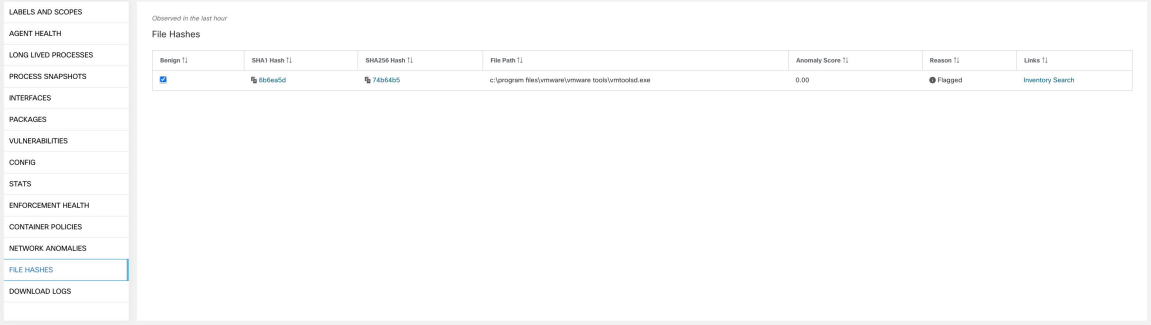
Cet onglet permet d'identifier les événements comportant des mouvements de données volumineux vers ou hors de cette charge de travail. Consultez Détection des anomalies de réseau basée sur le PCR pour obtenir plus de renseignements.

Figure 234: Anomalie de réseau de la charge de travail

Onglet Condensés de fichiers

Cet onglet détecte les anomalies de condensé de processus en évaluant la cohérence des condensés binaires de processus dans le système. Consultez la section Process hash anomaly detection pour en savoir plus.

Figure 235: Condensés de fichiers de charge de travail



Paquets logiciels

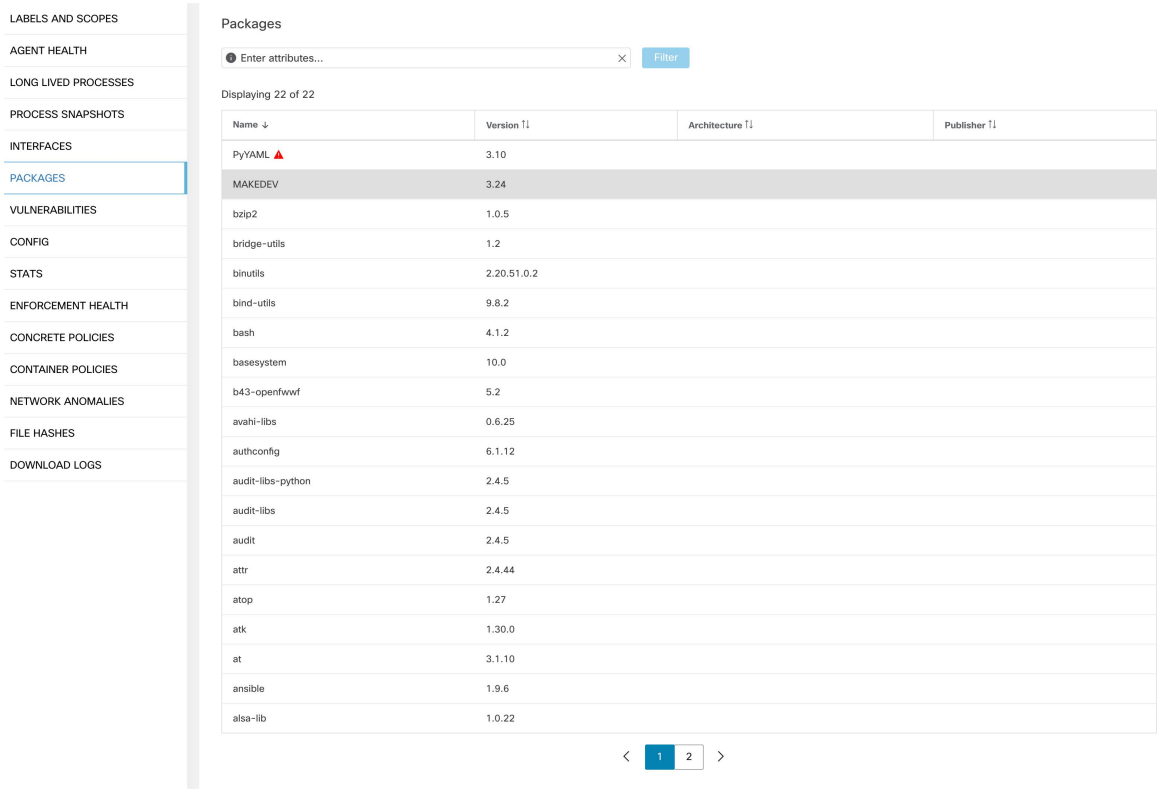
La fonctionnalité **Paquets logiciels** permet de visualiser les paquets installés sur les hôtes et les vulnérabilités qui les affectent. Plus précisément, elle permet de :

- Afficher les paquets enregistrés avec les gestionnaires de paquets suivants :
  - Linux : Gestionnaire de paquet RedHat (RPM) et gestionnaire de paquet Debian (dpkg)
  - Windows : Service de registre de Windows
- Afficher les vulnérabilités et expositions courantes (CVE) affectant les paquets installés sur un hôte.
- Définir des filtres d'inventaire en utilisant le nom et la version du paquet.

Onglet Packages (Logiciels)

Pour afficher les paquets installés sur un hôte, accédez à l'onglet Paquets sur la page Profil de la charge de travail du profil de charge de travail.

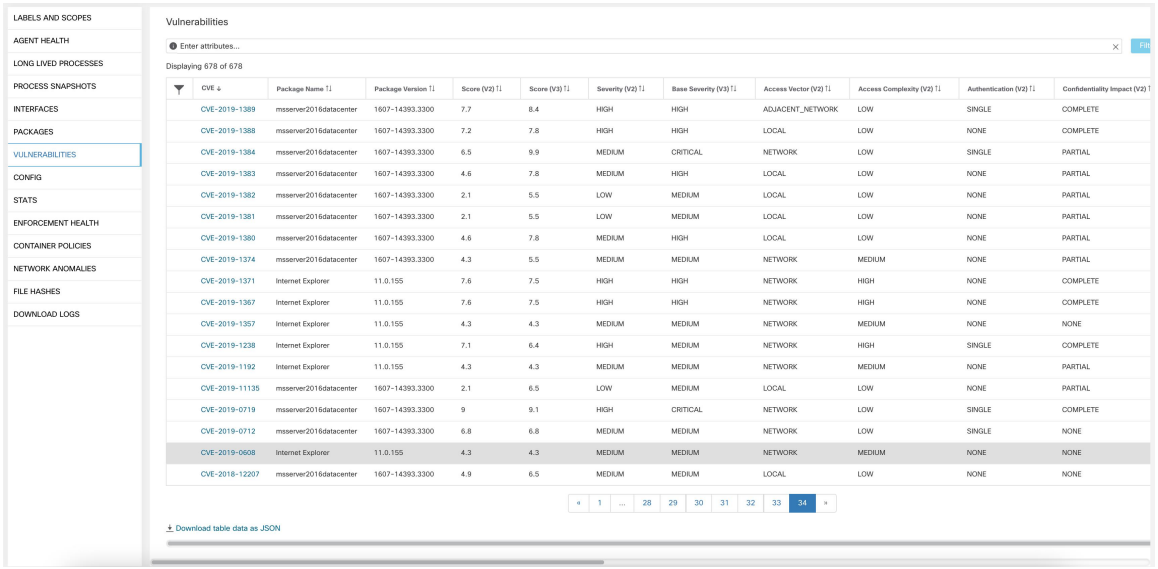
Figure 236: Paquets de profils de la charge de travail



Vulnérabilités et risques courants (CVE)

En plus d'afficher les paquets sous l'onglet Packages (paquets logiciels), nous affichons les vulnérabilités courantes qui les affectent ainsi que leur gravité. Chaque vulnérabilité contient un lien vers la base de données sur les vulnérabilités du pays (NVD) qui fournit des informations supplémentaires sur la vulnérabilité en question. En plus d'afficher l'ID CVE, nous affichons également la note d'impact (sur une échelle de 10), ce qui indique la gravité de la vulnérabilité.

Figure 237: CVE de paquets de profils de la charge de travail



Paquets Windows et CVE

La section suivante répertorie le comportement de l'agent Windows en ce qui concerne la transmission d'informations sur le paquet à Cisco Secure Workload.

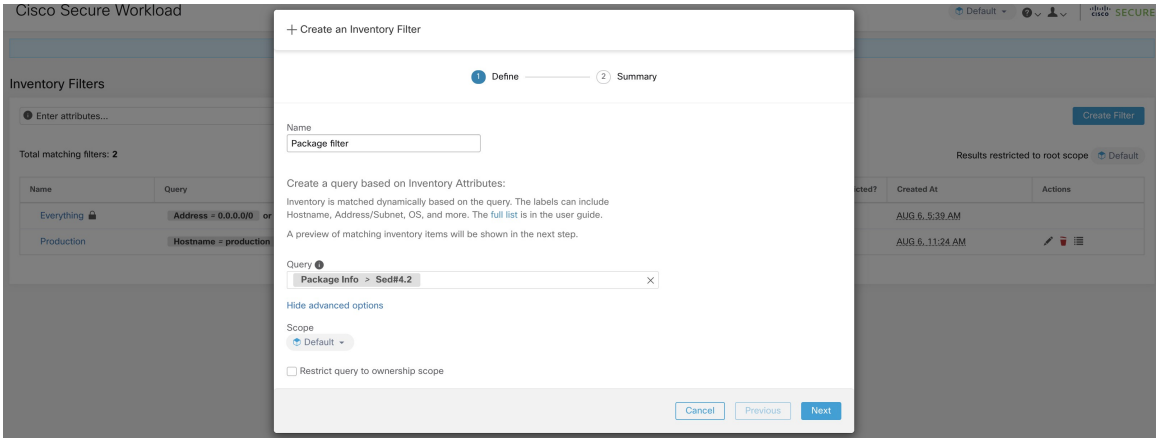
- Les applications Windows, PowerShell et IE sont présentées comme des paquets. .net Framework est également signalé en tant que paquet.
- Les autres applications Windows comme notepad.exe, cmd.exe, mstsc.exe, etc. ne sont pas signalées.
- Les rôles et les fonctionnalités configurés par un serveur Windows sont signalés en tant que paquets, mais la version peut être incorrecte. Par exemple : si le serveur DNS est configuré, la version signalée sera 0 ou 8.
- L'agent Windows signale les produits tiers installés à l'aide du programme d'installation de MSI ou du programme d'installation exe :
  - Pour les programmes d'installation MSI, les API MSI sont utilisées pour récupérer des informations sur le paquet. Par exemple, la version, le serveur de publication ou le nom du paquet.
  - Si le programme d'installation exe est utilisé pour installer le paquet, les informations sur le paquet sont extraites du registre.
  - Les champs du programme d'installation du paquet comme la version et le serveur de publication sont facultatifs. Si la version est manquante, le paquet ne sera pas signalé.
  - Si un produit est extrait du fichier compressé ou installé en tant qu'application, il ne sera pas signalé dans la liste des paquets.

Filtres d'inventaire

Il est possible de rechercher des informations relatives au paquet en définissant un filtre d'inventaire avec le nom et la version du paquet (facultatif).

La syntaxe de ce filtre est la suivante : PackageName#PackageVersion

Figure 238: Ensemble d'inventaire



Les opérations suivantes sont prises en charge :

- Equality (Égalité) : renvoie les hôtes avec les paquets correspondant à PackageName et à PackageVersion (si fourni).
- Inequality (Inégalité) : renvoie les hôtes avec les paquets correspondant à PackageName mais pas à PackageVersion (si fourni).
- Greater Than (Supérieur à) : renvoie les hôtes avec des paquets correspondant à PackageName et avec une version supérieure à PackageVersion.
- Greater Than or Equal To (Supérieur ou égal à) : renvoie des hôtes avec des paquets correspondant à PackageName et avec une version supérieure ou égale à PackageVersion.
- Less Than (inférieur à) – renvoie les hôtes avec les paquets correspondant à PackageName et avec une version antérieure à PackageVersion.
- Less Than or Equal To (Inférieur ou égal à) : renvoie les hôtes avec des paquets correspondant à PackageName et avec une version inférieure ou égale à PackageVersion.

Visibilité des données de vulnérabilité

La fonctionnalité de **visibilité des données de vulnérabilités** permet de détecter et d'afficher les vulnérabilités qui affectent les paquets et les processus sur un hôte. Les filtres d'inventaire peuvent être définis à l'aide :

des ID des CVE `des notes CVSS v2 et v3.- du vecteur d'accès et complexité d'accès CVSS v2.- du vecteur d'attaque CVSS v3, complexité de l'attaque et privilège requis.`

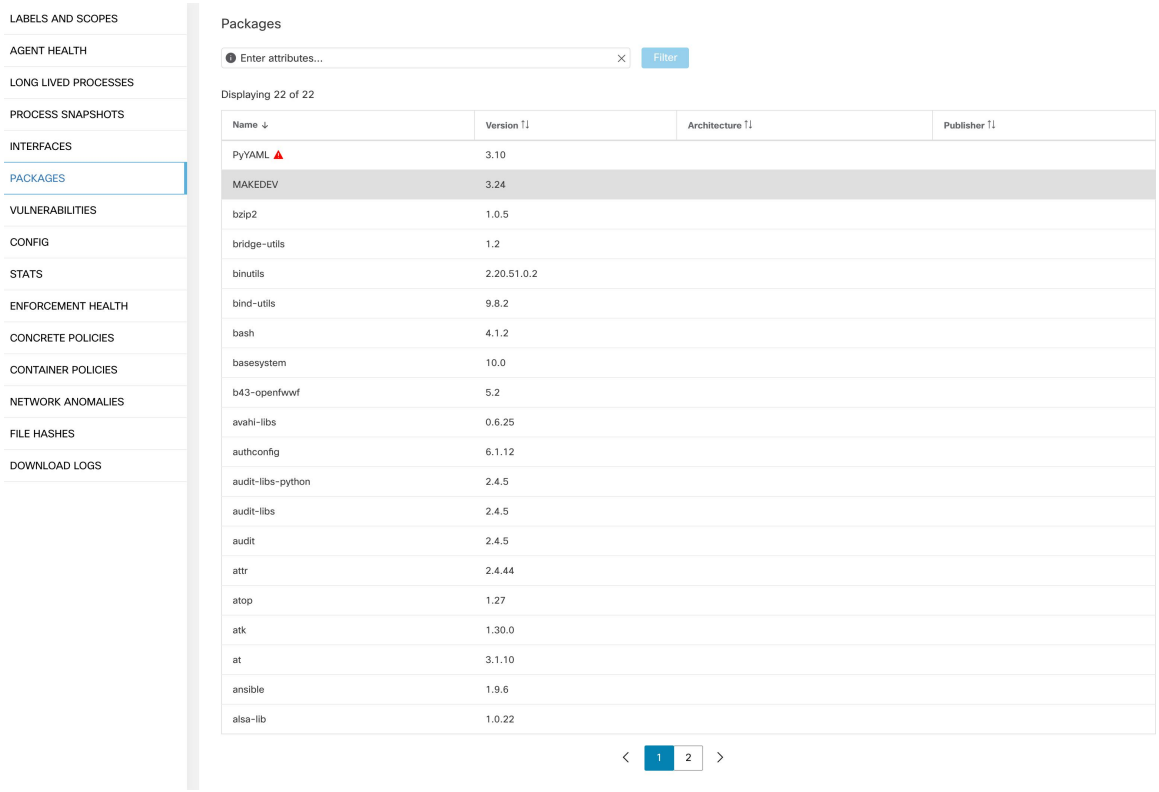
Profil de la charge de travail

Les renseignements sur les vulnérabilités qui affectent les paquets et les processus sur un système sont affichés sur la page Profil de la charge de travail (Profil de charge de travail).

Onglet Packages (Logiciels)

L'onglet des paquets répertorie les paquets installés sur un hôte et les vulnérabilités qui les affectent.

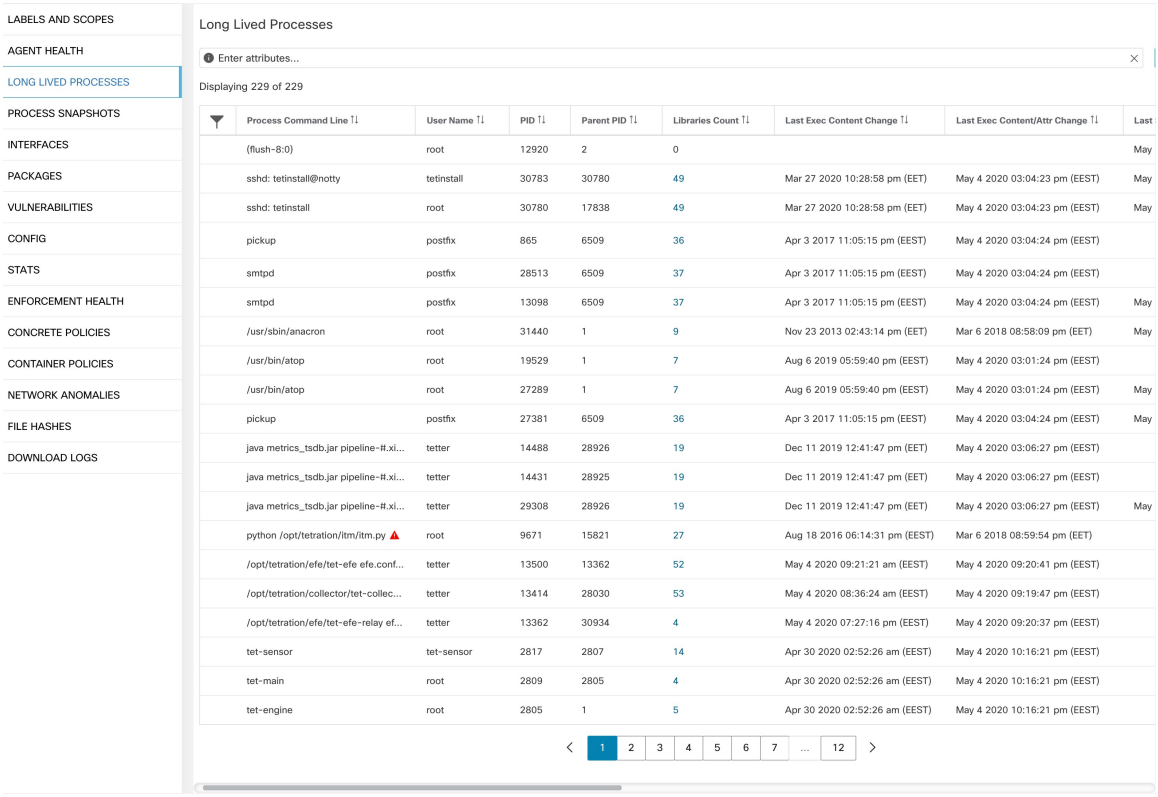
Figure 239: Paquets de profils de la charge de travail



Onglet Liste de processus

Les processus de longue durée sont affichés sous l'onglet de liste des processus.

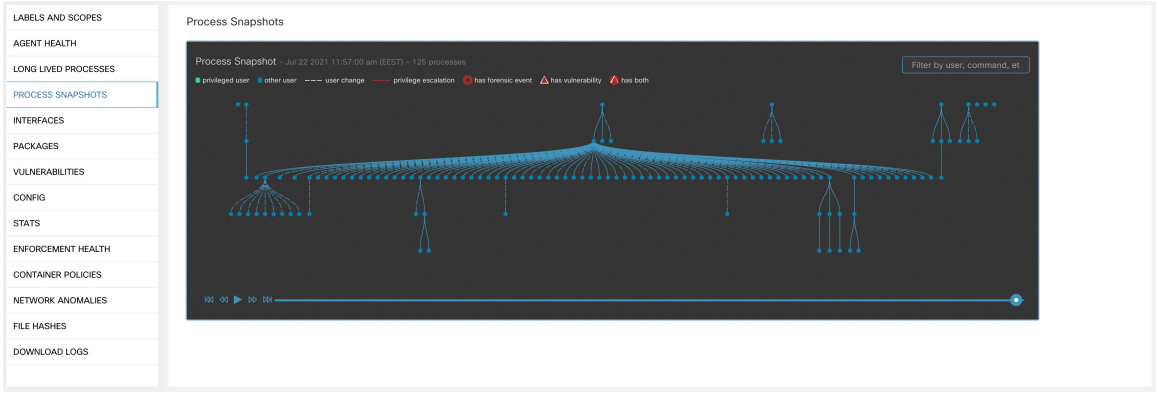
Figure 240: Liste des processus de profil de charge de travail



Onglet Process Snapshot (Instantané du processus)

Des informations sur les vulnérabilités sont affichées pour tous les processus de l'arborescence des processus sous l'onglet d'instantanés de processus.

Figure 241: Onglet d'instantané du processus de profil de charge de travail



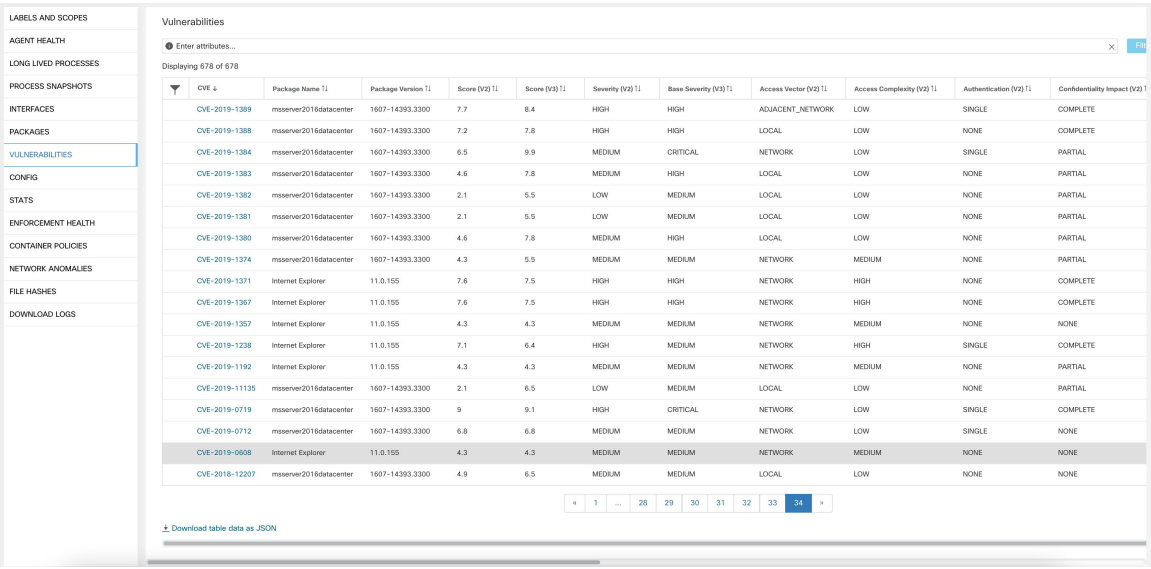
Onglet Vulnerabilities (Vulnérabilités)

L'onglet Vulnérabilités affiche la liste des vulnérabilités observées dans la charge de travail.

Pour chaque CVE, en plus des mesures d'impact de base, des informations sur les exploits basées sur nos informations sur les menaces sont affichées :

- Nombre d'exploits : nombre de fois où la CVE a été constatée exploitée de manière incontrôlée au cours de l'année écoulée
- Dernier exploit : la dernière fois que l'exploitation de la CVE de manière incontrôlée a été constatée par nos services de renseignement sur les menaces.

Figure 242: Onglet Vulnérabilités du profil de charge de travail



Filtres d'inventaire

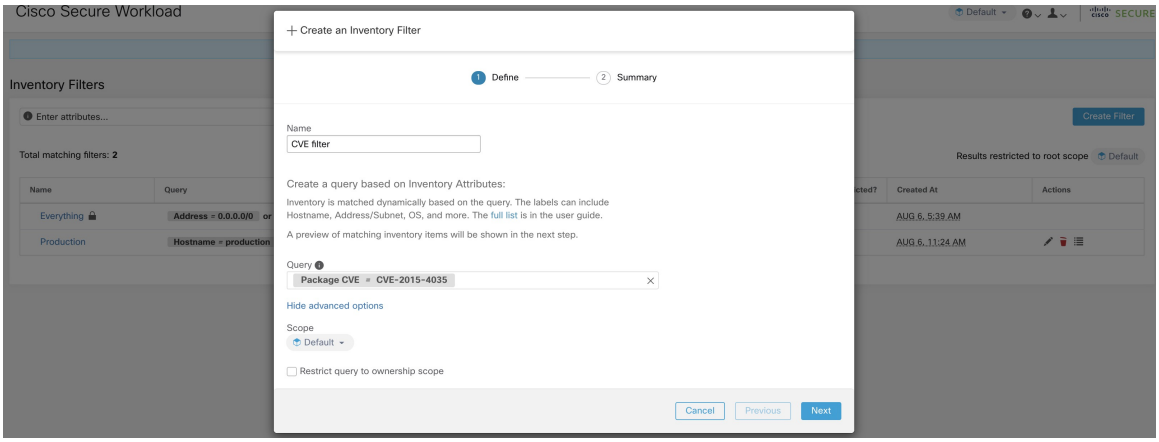
Les types de filtres d'inventaire suivants peuvent être définis pour identifier les hôtes comportant des paquets vulnérables :

Filtre basé sur l'ID CVE

Ce filtre permet de rechercher les hôtes concernés par un CVE spécifique ou n'importe quel CVE.

Pour rechercher un hôte affecté par un CVE spécifique, fournissez l'ID CVE au format : CVE-XXXX-XXXX

Figure 243: CVE de Filtre d'inventaire



Les opérations suivantes sont prises en charge :

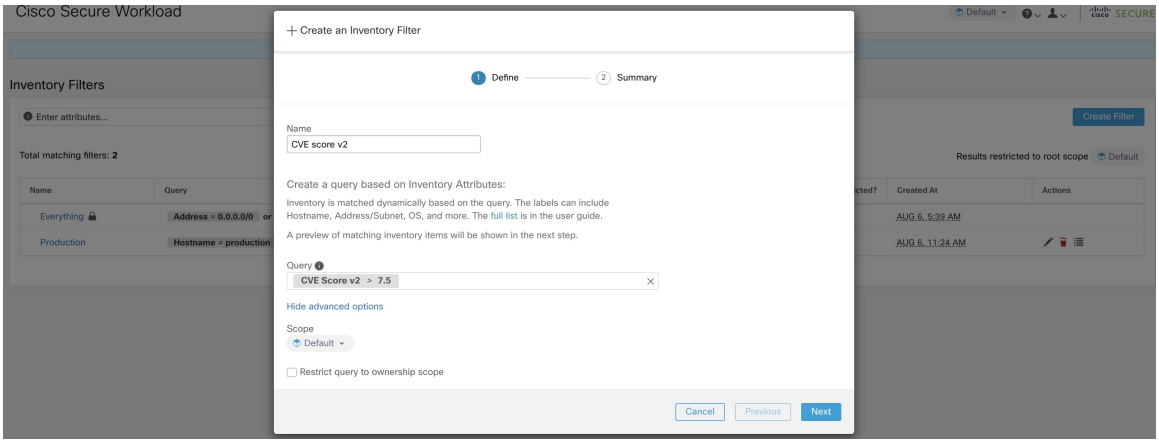
- Equality (Égalité) : renvoie les hôtes avec les paquets affectés par un ID CVE.
- Inequality (Inégalité) : renvoie les hôtes avec des paquets non affectés par un ID CVE.
- Contient (contains) renvoie les hôtes avec des paquets affectés par un CVE dans la chaîne d'entrée (la saisie de « cve » renverra les hôtes affectés par un CVE).
- Doesn't contain (Ne contient pas) : renvoie les hôtes avec des paquets non affectés par un CVE présent dans la chaîne d'entrée (la saisie de « cve » renverra les hôtes non affectés par un CVE).

Filtre basé sur la note d'impact CVSS (Common Vulnerabilities Scoring System, Système commun de notation des vulnérabilités)

Ce filtre permet de rechercher des hôtes qui ont un CVE avec le score d'impact CVSSv2 ou CVSSv3 spécifiée. Pour rechercher des hôtes qui ont des CVE avec une note d'impact (v2 ou v3), l'utilisateur peut fournir la note en format numérique.

Pour rechercher des hôtes qui ont un score d'impact CVE avec CVSSv2 supérieur à 7,5.

Figure 244: Filtre d'inventaire CVSS



Les opérations suivantes sont prises en charge :

- Égalité : renvoie les hôtes qui ont un CVE avec des notes d'impact CVSSv2 ou CVSSv3 spécifiées.
- Inégalité : renvoie des hôtes qui n'ont pas de CVE avec des notes d'impact CVSSv2 ou CVSSv3 spécifiées.
- Supérieur à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont supérieures aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Supérieur ou égal à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont supérieures ou égales aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Inférieur à : renvoie les hôtes dont les notes d'impact CVE avec CVSSv2 ou CVSSv3 sont inférieures aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.
- Inférieur ou égal à : renvoie les hôtes dont les scores d'impact CVE avec CVSSv2 ou CVSSv3 sont inférieures ou égales aux notes d'impact CVSSv2 ou CVSSv3 spécifiées, respectivement.

Filtres basés sur CVSSv2

Des filtres d'inventaire peuvent être créés en utilisant les vecteurs d'accès et les complexités d'accès pour identifier les hôtes vulnérables. Ces filtres prennent en charge les types d'opérations suivants :

- Equality (Égalité) : renvoie des hôtes avec des paquets affectés par des vulnérabilités correspondant au filtre.
- Inequality (Inégalité) : renvoie des hôtes avec des paquets non affectés par des vulnérabilités correspondant au filtre.

Vecteur d'accès

Le vecteur d'accès reflète la façon dont la vulnérabilité est exploitée. Plus l'agresseur peut s'éloigner du système vulnérable, plus la note de base est élevée. Le tableau ci-dessous répertorie les différents vecteurs d'accès avec leurs exigences d'accès :

Valeur	Type d'accès
LOCAL	Physique ou local (shell).
RÉSEAU_ADJACENT	Diffusion ou collision.
RÉSEAU	Exploitable à distance.

Complexité de l'accès

Cette mesure mesure la complexité de l'exploitation d'une vulnérabilité une fois que l'agresseur est en mesure d'accéder au système cible. La note de base est inversement proportionnelle à la complexité de l'accès. Les différents types de complexité d'accès sont les suivants :

Valeur	Description
ÉLEVÉE	Il existe des conditions d'accès spécialisées.
MOYENNE	Les conditions d'accès sont quelque peu spécialisées.

Valeur	Description
FAIBLE	Il n'existe pas de conditions d'accès spécifiques.

Filtres basés sur CVSSv3

Les vecteurs d'attaque, la complexité des attaques et les privilèges requis pour influencer la note CVSSv3 et qui peuvent être utilisés dans les filtres d'inventaire. Ces filtres prennent en charge les opérations suivantes :

- Equality (Égalité) : renvoie des hôtes avec des paquets affectés par des vulnérabilités correspondant au filtre.
- Inequality (Inégalité) : renvoie des hôtes avec des paquets non affectés par des vulnérabilités correspondant au filtre.

vecteur d'attaque

Cette mesure reflète le contexte dans lequel l'exploitation des vulnérabilités est possible. Plus un attaquant peut être éloigné du composant vulnérable, plus la note de base est élevée. Le tableau ci-dessous répertorie les différents vecteurs d'attaque avec leurs exigences d'accès :

Valeur	Type d'accès
LOCAL	Local (clavier, console) ou distant (SSH).
PHYSIQUE	Un accès physique est nécessaire.
RÉSEAU_ADJACENT	Diffusion ou collision.
RÉSEAU	Exploitable à distance.

Complexité de l'attaque

Cette mesure décrit les conditions qui doivent être réunies pour exploiter la vulnérabilité. La note de base est la plus élevée pour les attaques les moins complexes. Les différents types de complexité d'accès sont les suivants :

Valeur	Description
ÉLEVÉE	Des efforts importants ont été nécessaires pour la configuration et l'exécution de l'attaque.
FAIBLE	Il n'existe pas de conditions d'accès spécifiques.

Privilèges requis

Cette mesure décrit le niveau de privilèges qu'un attaquant doit posséder avant d'exploiter avec succès la vulnérabilité. La note de base est la plus élevée lorsque des privilèges ne sont pas nécessaires pour mener une attaque. Les différentes valeurs de privilège nécessaires sont les suivantes :

Valeur	Privilèges requis
ÉLEVÉE	Privilèges fournissant un contrôle important sur le composant vulnérable.
FAIBLE	Des privilèges faible qui accordent l'accès à des ressources non sensibles.
AUCUN	Aucun privilège n'est nécessaire pour effectuer une attaque.

Profil de service

Cisco Secure Workload offre une visibilité sur tous les services Kubernetes et autres équilibreurs de charge intégrés par un orchestrateur externe. La page de profil de service affiche les détails d'un service donné.

Note La page du profil de service est accessible à partir de différents endroits. L'une des façons d'afficher un profil de service consiste à rechercher un service comme décrit dans la section de recherche

Dans les résultats de la recherche, cliquez sur le nom d'un service sous l'onglet Services pour accéder à son profil. Les informations suivantes sont disponibles pour le service :

En-tête

L'en-tête comprend :

- **Nom de l'orchestrateur :** nom de l'orchestrateur externe qui a signalé ce service.
- **Type d'orchestrateur :** type de l'orchestrateur externe.
- **Espace de nom :** espace de nom du service.
- **Type de service :** type de service. Les valeurs possibles comprennent ClusterIP, Node, Port et LoadBalancer.

Adresses IP et ports

Ce tableau répertorie toutes les combinaisons possibles d'adresses IP et de ports grâce auxquelles ce service est accessible. Pour les services de type NodePort, ce tableau affiche les associations ClusterIP:Port et NodeIp:NodePort.

Étiquettes d'utilisateur

La liste des étiquettes téléversées par les utilisateurs et générées par le système par l'orchestrateur pour ce service.

Portées

Liste des portées auxquelles l'ensemble appartient.

Profil de Pod

Cisco Secure Workload offre une visibilité de tous les pods Kubernetes acquis par un orchestrateur externe Kubernetes. La page de profil de pod affiche les détails d'un pod donné.

Note La page de profil du pod est liée à plusieurs emplacements. L'une des façons d'afficher un profil de pod consiste à rechercher un pod comme décrit dans la section de recherche

Dans les résultats de la recherche, cliquez sur le nom d'un pod sous l'onglet Pods pour accéder à son profil. Les informations suivantes sont disponibles pour le pod :

En-tête

L'en-tête comprend :

- **Orchestrator Name :** nom de l'orchestrateur externe qui a signalé ce pod.
- **Type d'orchestrateur :** type de l'orchestrateur externe.
- **Espace de nom :** espace de nom du pod.
- **IP Address : adresse** IP du pod.

Étiquettes d'utilisateur

La liste des étiquettes téléversées par les utilisateurs et générées par le système par l'orchestrateur pour ce pod.

Portées

Liste des portées à laquelle le service appartient.

Container Vulnerability Scanning

It is recommended to regularly scan Kubernetes pods for vulnerabilities to maintain the health and identify potential security weaknesses.

Prerequisites

- Ensure that a Kubernetes cluster is on board.
- Ensure that the CSW Kubernetes daemonset agent is installed as part of the Kubernetes cluster.

Procedure

Étape 1 Navigate to **Manage** > **Workloads** > **Kubernetes**.

Note All onboarded clusters are displayed under **Clusters** along with the associated inventory, such as services and pods.

Étape 2 Click **Pod Vulnerability Scanning**.

Étape 3 Enable the toggle under **Actions** to start the scan. By default, the toggle is disabled.

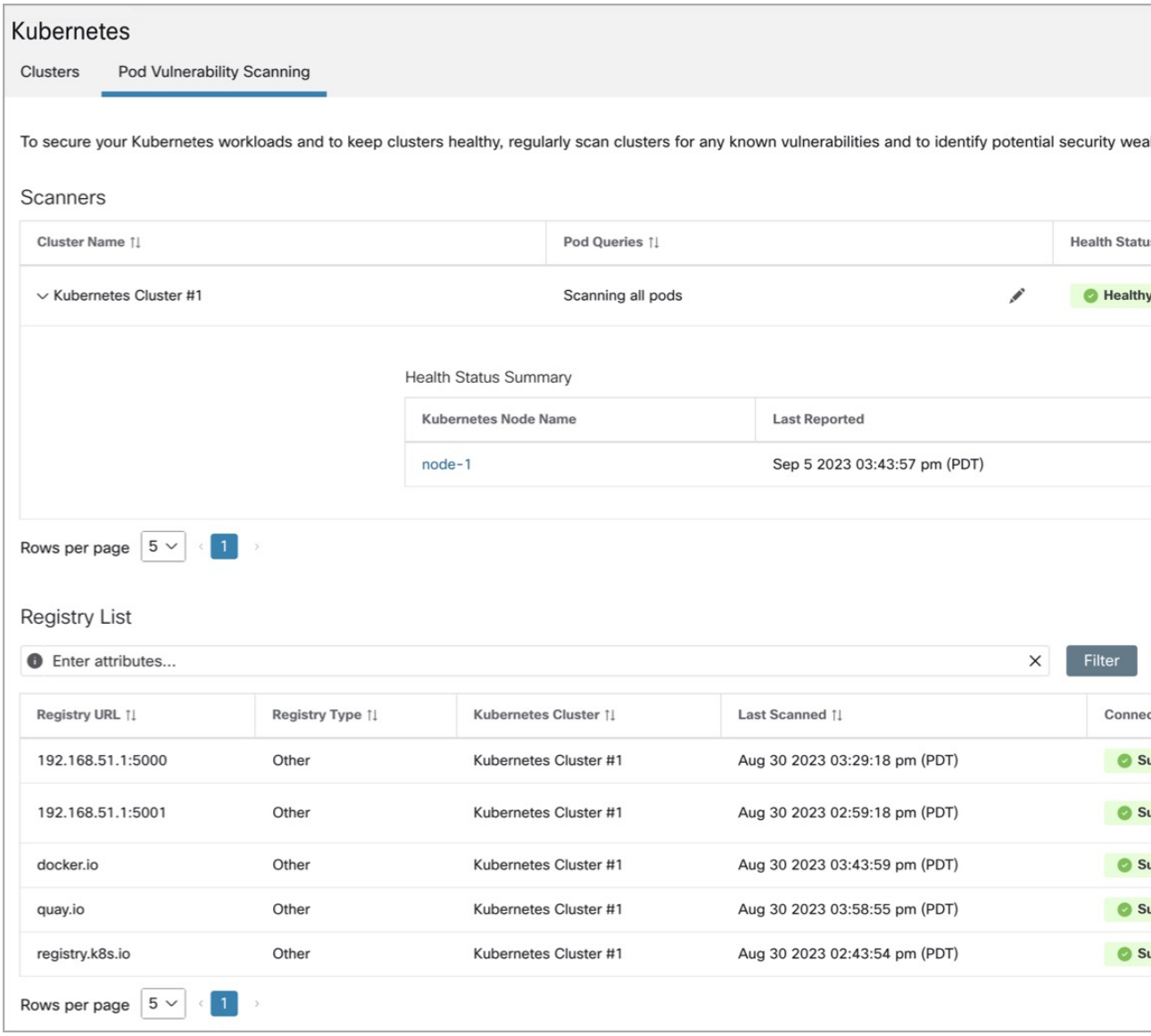
Étape 4 Click the edit icon to modify the query and select a subset of pods running on the cluster.

Note
- By default, a pod query is populated to scan all pod inventories running in the cluster. However, you can edit pod queries to select the pods to scan.
- Currently, scanning of Windows container images is not supported.

Étape 5 Expand a cluster to view the **Health Status Summary**.

- Clicking on a Kubernetes Node Name navigates you to Workload Profile.
- Enabling the toggle automatically downloads addititional information to the host so that the scanner can execute.

Figure 245: Pod Vulnerability Scanning



Étape 6 Verify the connection status and enter credentials, if required. All registries that are detected are displayed in **Registry List**.

Note Credentials may vary based on the registry enter.

Registry Type	Credentials
Azure	Tenant ID, Client ID, Secret Key
AWS	Access Key, Secret Key
GCP	Service account key in JSON format
Other	Username, Password

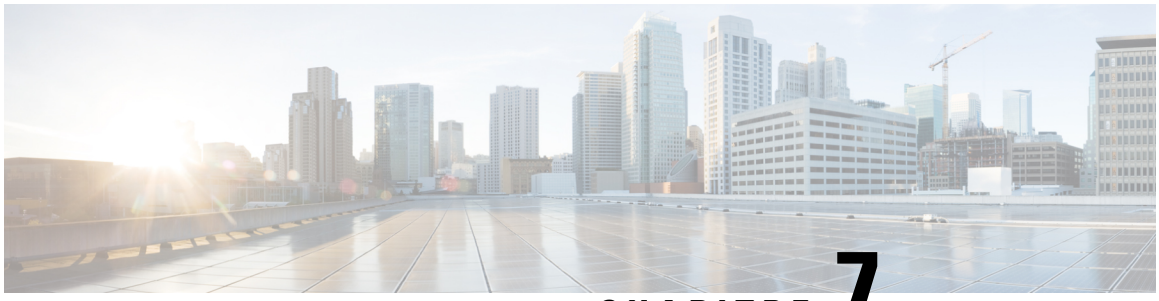
Troubleshooting

For the connection to be successful, ensure that the following conditions are met:

a. The scanner pod is able to connect to the registry.

b. The required network policies are in place.

c. Credentials are entered, if required.



CHAPITRE 7

Gérer le cycle de vie des politiques dans Cisco Secure Workload

Principes de base de la politique de segmentation

Le but des politiques de segmentation et de microsegmentation est de n'autoriser que le trafic dont votre entreprise a besoin pour ses activités et de bloquer tout le reste. L'objectif est de réduire la surface d'attaque de votre réseau sans perturber les tâches opérationnelles.

Les politiques de segmentation de Cisco Secure Workload autorisent ou bloquent le trafic en fonction de sa source, de sa destination, de son port, de son protocole et de quelques autres attributs qui sont généralement propres à la plateforme.

Vous pouvez créer des politiques manuellement et utiliser la puissante fonctionnalité de découverte automatique des politiques de Cisco Secure Workload pour générer d'autres politiques en fonction du trafic réseau existant.

Vous pouvez passer en revue, affiner et analyser vos politiques, puis les appliquer lorsque vous êtes sûr qu'elles n'autorisent que le trafic dont votre entreprise a besoin.

Important La microsegmentation crée essentiellement un pare-feu autour de chaque charge de travail.

Par conséquent, pour que le trafic passe entre chaque paire client-fournisseur, les deux extrémités de la conversation doivent autoriser la conversation : le client et le fournisseur doivent chacun avoir une politique autorisant le trafic.

Remarque Les termes *règle de pare-feu*, *périphérie* et *périphérie de grappe* sont parfois utilisés pour signifier « politique ».

Utiliser des espaces de travail pour gérer les politiques

Les espaces de travail (anciennement « espaces de travail d'applications » ou « applications ») sont les endroits où vous travaillez et gérez les politiques.

Vous pouvez effectuer toutes les activités liées aux politiques pour une portée particulière, telles que la création, l'analyse et l'application des politiques, dans l'espace de travail ou les espaces de travail associés à cette portée.

Chaque espace de travail constitue un environnement indépendant, permettant des expérimentations sans effet sur les autres espaces de travail.

Contrôle de l'accès des utilisateurs aux espaces de travail

Les espaces de travail sont destinés à être utilisés par plusieurs utilisateurs de la même équipe en tant que documents partagés.

Pour contrôler l'accès à un espace de travail, attribuez des rôles d'utilisateur pour la portée associée à l'espace de travail. Pour en savoir plus, consultez la section Rôles.

Utilisation des politiques : Accès à la page des espaces de travail

- **Pour utiliser les politiques, afficher les espaces de travail d'application existants ou en créer de nouveaux :**

  Choisissez **Defend (Défendre)** > **Segmentation (Segmentation)** dans la barre de navigation à gauche de la fenêtre.

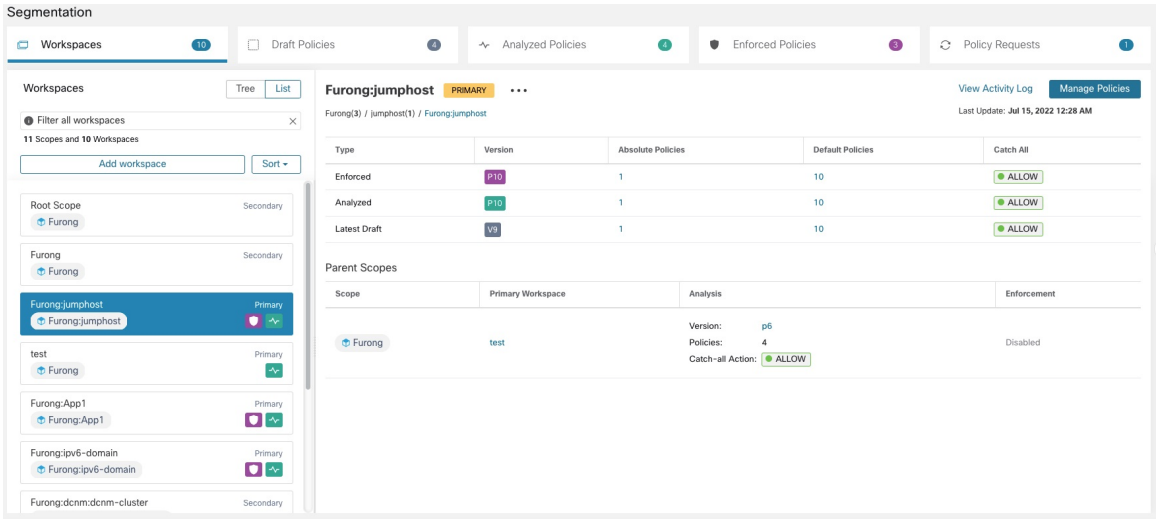
- **Pour afficher un espace de travail en particulier :**

  Dans la liste des portées sur le côté gauche de la page Workspaces (Espaces de travail), accédez à la portée associée à l'espace de travail, puis cliquez sur ce dernier. L'espace de travail actif actuel est mis en surbrillance dans la liste.

- **Si vous êtes à la recherche d'un espace de travail et que vous souhaitez revenir à la liste des espaces de travail :**

  Cliquez sur le lien **Workspaces** (Espaces de travail) près du côté gauche de la page que vous examinez.

Figure 246: Page Workspace Management (Gestion de l'espace de travail)



Créer un espace de travail

Pour créer des politiques pour une portée, créez d'abord un espace de travail pour cette dernière.

Pour créer un espace de travail :

1. Dans le menu de navigation sur le côté gauche de la fenêtre, choisissez **Defend (Défendre)** > **Segmentation (Segmentation)**.
2. Dans la liste des portées située à gauche de la page, recherchez la portée pour laquelle vous souhaitez créer des politiques ou faites défiler l'écran jusqu'à cette portée.
3. Passez le curseur sur la portée jusqu'à ce qu'un signe Plus bleu s'affiche, puis cliquez dessus.
4. Remplissez le formulaire et cliquez sur **Create** (Créer) lorsque vous avez terminé.

S'il existe un espace de travail pour la portée, tout espace de travail supplémentaire est créé en tant qu'espace de travail secondaire.

Espaces de travail principal et secondaire

Pour chaque portée, vous pouvez créer un espace de travail principal et plusieurs espaces de travail secondaires.

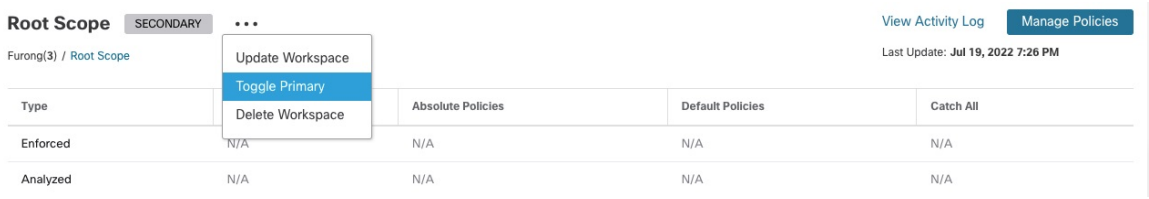
Seul un espace de travail principal peut être mis en application. Parmi les autres fonctionnalités disponibles uniquement pour les espaces de travail principaux, citons la possibilité de gérer des politiques dans lesquelles le consommateur et le fournisseur résident dans des portées différentes, l'analyse en direct des politiques, les rapports de conformité et la définition collaborative des politiques de sécurité.

Utilisez des espaces de travail secondaires pour essayer les politiques lorsque vous souhaitez conserver les politiques existantes dans l'espace de travail principal.

Pour faire d'un espace de travail un espace de travail principal ou secondaire :

Vous pouvez faire basculer un espace de travail de principal à secondaire et inversement à tout moment en cliquant sur l'icône de menu à côté du nom de l'espace de travail en haut de la page et en sélectionnant **Toggle Primary**(basculer l'espace de travail principal).

Figure 247: Commutation d'un espace de travail entre principal et secondaire



Renommer un espace de travail

Pour renommer un espace de travail :

Cliquez sur le ••• côté du type d'espace de travail (principal ou secondaire) affiché près du haut de la page et choisissez **Update Workspace** (Mettre à jour l'espace de travail).

Afficher les charges de travail d'une portée

Dans n'importe quel espace de travail, cliquez sur l'onglet **Matching Inventories** (Inventaires correspondants).

Rechercher dans un espace de travail

Pour rechercher dans un espace de travail des charges de travail, des grappes ou des politiques :

1. Sélectionnez **Defend (Défendre)** > **Segmentation (Segmentation)**.
2. Dans la liste des portées sur la gauche, cliquez sur la portée et l'espace de travail qui vous intéressent.
3. Cliquez sur **Manage Policies** (Gestion des politiques).
4. Cliquez sur la loupe.
5. Saisissez les critères de recherche

Critères de recherche

Plusieurs critères sont traités comme ET logique.

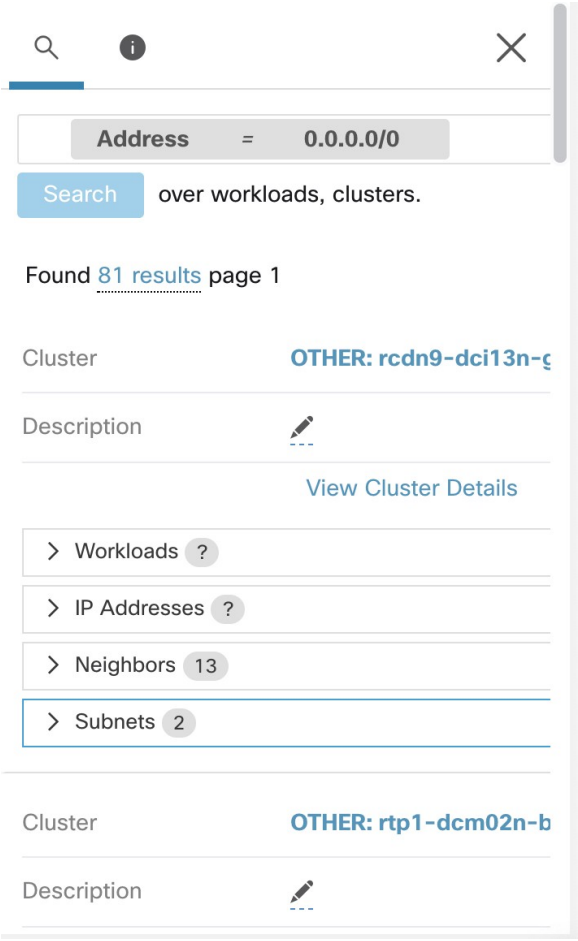
Pour les adresses IP et les valeurs numériques :

- Indiquez le OU logique à l'aide d'une virgule : « port: 80,443 ».
- Les requêtes de plage sont également prises en charge pour les valeurs numériques : « port : 3000-3999 ».

Filtres	Description
Nom	Saisissez un nom de grappe ou de charge de travail. Effectue une recherche de sous-chaîne sensible à la casse.

Filtres	Description
Description	Recherche les descriptions des grappes.
Approuvé	Correspond aux groupes approuvés en utilisant les valeurs « vrai » ou « faux ».
Address (adresse)	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux charges de travail ou aux grappes qui recoupent ce sous-réseau.
Super-réseau	Saisissez un sous-réseau en notation CIDR (par exemple, 10.11.12.0/24) pour correspondre aux grappes dont les charges de travail sont entièrement contenues dans ce sous-réseau.
Processus	Recherche les processus de charge de travail à l'aide de la recherche de sous-chaîne sensible à la casse.
UID de processus	Recherche les noms d'utilisateurs des processus de charge de travail.
Port	Recherche à la fois le port du fournisseur de charge de travail et le port de la politique.
Protocol	Recherche à la fois le protocole du fournisseur de charge de travail et le protocole de politique.
Consumer Name	Correspond au nom de la grappe de consommateurs d'une politique. Effectue une correspondance de sous-chaîne sensible à la casse.
Provider Name	Correspond au nom de la grappe de fournisseurs d'une politique. Effectue une correspondance de sous-chaîne sensible à la casse.
Adresse du client	Correspond aux politiques dont l'adresse du client recouvre l'adresse IP ou le sous-réseau fournis.
Adresse du fournisseur	Correspond aux politiques dont l'adresse de fournisseur recouvre l'adresse IP ou le sous-réseau fournis.

Exemple de recherche

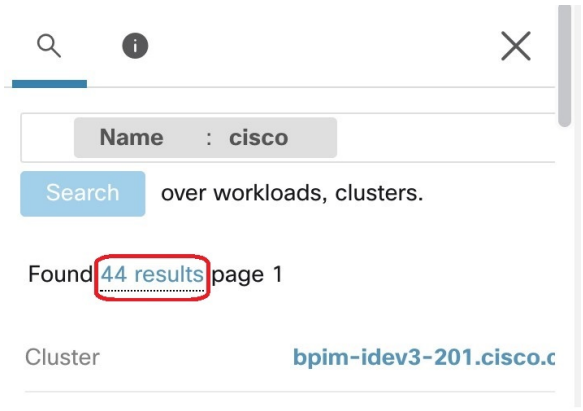


Filtrage des résultats de la recherche pour un type spécifique

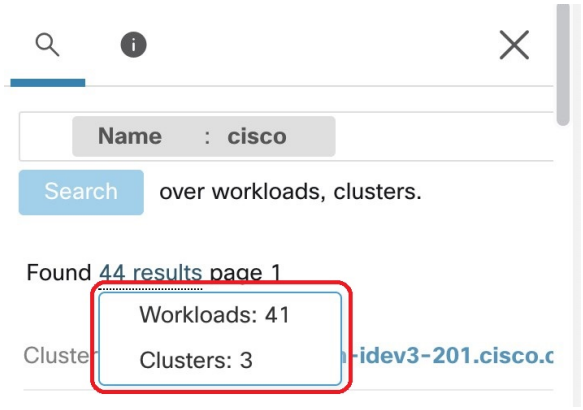
Les résultats de la recherche peuvent inclure plusieurs types d'objets, par exemple des charges de travail et des grappes.

Pour filtrer les résultats de la recherche pour un type spécifique :

1. Cliquez sur le total du résultat :



2. Sélectionnez le type dans la liste déroulante :



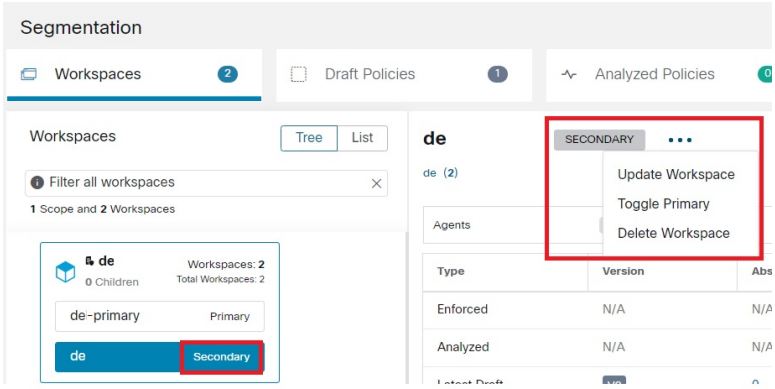
3. Un filtre de type sera ajouté et la recherche sera réexécutée.

Suppression d'espaces de travail

Seuls les espaces de travail secondaires (non principaux) peuvent être supprimés. Pour faire passer un espace de travail au niveau secondaire, consultez Espaces de travail principal et secondaire, on page 431.

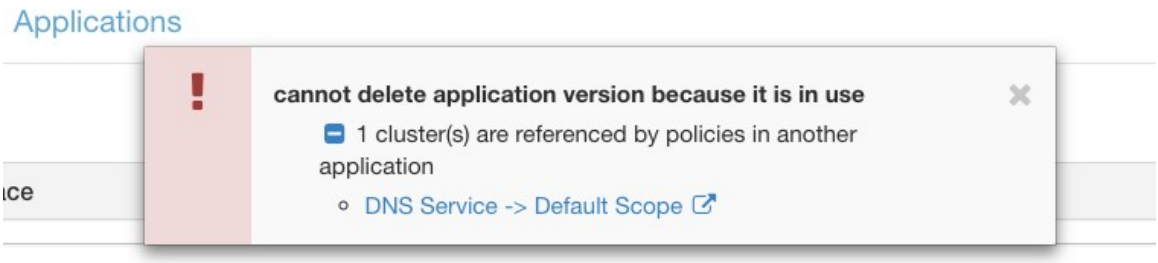
Pour supprimer un espace de travail :

1. Choisissez **Defend (défense) > Segmentation (segmentation).**
2. Dans la liste des portées sur le côté gauche de la page, accédez à la portée contenant l'espace de travail à supprimer et cliquez dessus.
3. Cliquez sur l'espace de travail à supprimer.
4. Cliquez sur le ••• à côté de **Secondary (Secondaire)** et choisissez **Delete Workspace** (Supprimer l'espace de travail).



Si une charge de travail ou une grappe dans un espace de travail est référencée par une politique dans un autre espace de travail à la suite d'un service fourni, l'espace de travail dépendant ne peut pas être supprimé et une liste des dépendances sera renvoyée. Ces informations peuvent être utilisées pour corriger la dépendance.

Figure 248: Liste des éléments empêchant la suppression de l'espace de travail



Dans de rares cas, il peut y avoir une dépendance croisée où l'espace de travail A dépend d'une grappe dans l'espace de travail B et un espace de travail B dépend d'une grappe dans l'espace de travail A. Dans ce cas, les politiques individuelles ou les versions de politiques publiées (p*) doivent être supprimées. L'erreur « delete restrictions » (restrictions de suppression) fournit des liens vers toutes les politiques permettant d'y parvenir.

Pour supprimer les versions p*, consultez Afficher, comparer et gérer les versions des politiques analysées, on page 556 ou Afficher, comparer et gérer les versions des politiques appliquées, on page 571.

À propos des politiques

Attributs de la politique

Table 23: Propriétés de la politique

Propriétés de la politique de sécurité	Description
Portée pour laquelle la politique est définie	Une politique a généralement une incidence uniquement sur les charges de travail qui sont membres de la portée associée à l'espace de travail dans lequel la politique est définie. (Cependant, consultez également les rubriques sous Aborder les complexités de la politique, on page 515). Pour en savoir plus, consultez Exemple de politique, on page 439.
Consommateurs	Le client d'un service ou l'initiateur d'une connexion. N'importe quel filtre de portée, de grappe ou d'inventaire peut être utilisé en tant que consommateur dans une politique. Consultez les informations importantes dans À propos du consommateur et du fournisseur dans les politiques, on page 439.
Fournisseur	Le serveur ou le destinataire d'une connexion. N'importe quel filtre de portée, de grappe ou d'inventaire peut être utilisé comme fournisseur dans une politique. Consultez les informations importantes dans À propos du consommateur et du fournisseur dans les politiques, on page 439.
Protocoles et ports	Le port (d'écoute) du serveur et le protocole IP du service mis à disposition par le fournisseur qui doivent être autorisés ou bloqués.
Action	ALLOW ou DENY : s'il faut autoriser ou abandonner le trafic du consommateur au fournisseur sur le port de service/protocole donné.
Rang et priorité	Pour en savoir plus sur le rang et la priorité des politiques dans un espace de travail, consultez Rang de politique : Absolue, Par défaut et Collectrice, on page 437.

Rang de politique : Absolue, Par défaut et Collectrice

Le rang de la politique détermine si une politique est remplacée par une politique plus spécifique inférieure dans la liste de priorité (ou dans une portée inférieure de l'arborescence des portées). La politique de priorité la plus basse de chaque portée est toujours la règle Collectrice.

Rang de la politique	Description
Absolue	Les politiques absolues prennent effet même si elles contredisent des politiques spécifiques à l'application situées à un niveau inférieur dans la liste des politiques (et donc moins prioritaires) ou dans des portées situées à un niveau inférieur dans l'arborescence des portées. En général, utilisez les politiques absolues pour appliquer les bonnes pratiques, protéger différentes zones ou charges de travail spécifiques à la mise en quarantaine. Par exemple, utilisez des politiques absolues pour contrôler le trafic vers les serveurs DNS ou NTP, ou pour répondre aux exigences réglementaires. Les politiques absolues sont répertoriées à un niveau supérieur à celui des politiques par défaut dans la liste de priorités des politiques.
Par défaut	Les politiques par défaut peuvent être remplacées par des politiques inférieures dans la liste des politiques ou dans des portées inférieures dans l'arborescence des portées. En général, les politiques précises sont des politiques par défaut. Les politiques par défaut sont répertoriées à un niveau inférieur à celui des politiques absolues dans la liste de priorités des politiques.
Collectrice	Chaque espace de travail est doté d'une politique collectrice fourre-tout qui gère le trafic dans chaque direction qui ne correspond à aucune politique explicitement spécifiée dans l'espace de travail. L'action Collectrice peut être Allow (autoriser) ou Deny(refuser). En général, définissez la politique Catch-All (Collectrice) comme suit : • **Allow**(Autoriser) le trafic dans les portées supérieures de l'arborescence, de sorte que les politiques des portées inférieures de l'arborescence puissent évaluer le trafic. • **Deny** (Refuser) le trafic au niveau de l'extrémité la plus précise, au bas de l'arborescence de la portée. Cela permet aux politiques de toutes les portées de l'arborescence de mettre en correspondance le trafic, tout en bloquant le trafic qui ne correspond à aucune politique d'aucune portée. La règle « collectrice » est appliquée à toutes les interfaces de chaque charge de travail dans l'espace de travail.

Héritage des politiques et arborescence de portée

Vos charges de travail étant organisées en une arborescence hiérarchique, vous pouvez créer des politiques générales une fois dans une portée située au sommet de l'arborescence ou à proximité, et les politiques peuvent éventuellement s'appliquer à toutes les charges de travail dans toutes les portées situées en dessous de cette portée dans l'arborescence.

Vous spécifiez si les politiques générales peuvent être remplacées par des politiques plus spécifiques, plus bas dans l'arborescence.

Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 437.

À propos du consommateur et du fournisseur dans les politiques

Le consommateur et le fournisseur précisés dans une politique servent aux fins suivantes :

- Ils précisent les charges de travail ou les agents Cisco Secure Workload qui reçoivent les règles de politique ou de pare-feu.
- Ils précisent l'ensemble d'adresses IP auxquelles les règles de pare-feu installées sur les charges de travail s'appliquent.

Si un hôte possède plusieurs interfaces (adresses IP), les politiques s’appliquent à toutes les interfaces.

Important Les éléments ci-dessus représentent le comportement par défaut de la programmation des règles de pare-feu sur les charges de travail. Si les adresses IP spécifiées dans les règles de pare-feu différentes des adresses IP des charges de travail sur lesquelles la politique est installée, vous devez séparer les deux objectifs des consommateurs et des fournisseurs dans une politique. Consultez Consommateur ou fournisseur réel, à la page 535.

Exemple de politique

L’exemple de politique suivant illustre l’importance de la portée dans laquelle une politique est définie, l’incidence de l’héritabilité des politiques et de l’utilisation de filtres d’inventaire pour créer des politiques spécifiques ou des politiques qui s’appliquent aux charges de travail dans plusieurs portées.

Considérons l’exemple suivant concernant trois portées :

- **`Applis`**

  et leurs portées enfants

  - **`Apps:HR`** et
  - **`Apps:Commerce`**

En outre, les filtres d’inventaire PRODUCTION et NON-PRODUCTION précisent respectivement les hôtes de production et les hôtes hors production. (Vous pouvez définir un filtre d’inventaire à appliquer aux hôtes dans une portée ou dans plusieurs).

Supposons que la politique suivante soit définie pour la portée **`Applications`** :

```
DENY PRODUCTION -> NON-PRODUCTION on TCP port 8000 (Absolute)
```

Étant donné qu’il s’agit d’une politique absolue définie dans l’espace de travail principal sous la portée **`Applications`**, elle affecte tous les hôtes DE PRODUCTION ET HORS DE PRODUCTION membres de la portée **`Applications`**, y compris les membres de ses portées descendantes (hôtes qui appartiennent aux environnements **`Apps:RH`** et **`Apps:Commerce`**).

Considérons maintenant le cas où exactement la même politique est définie dans l’espace de travail associé à la portée **`Apps:HR`**. Dans ce scénario, la politique ne peut affecter que les hôtes PRODUCTION ET NON-PRODUCTION membres de la portée **`Apps:HR`**. Plus précisément, cette politique fait en sorte que les règles d’entrée sur les hôtes RH NON PRODUCTION (le cas échéant) refusent les connexions sur le port TCP 8000 à partir de **n’importe quel** hôte PRODUCTION, et les règles sortantes sur les hôtes de

PRODUCTION RH (le cas échéant) abandonnent les demandes de connexion vers **tout** hôte HORS-PRODUCTION.

Créer et découvrir des politiques

Bonnes pratiques pour la création de politiques

- Pour une présentation de l'ensemble du processus de segmentation, consultez Premiers pas avec la segmentation et la microsegmentation, à la page 2 et les sous-rubriques.
- Créez manuellement des politiques qui s'appliquent globalement à votre réseau.

  Par exemple, bloquez le trafic indésirable vers vos charges de travail provenant de l'extérieur de votre réseau ou mettez les hôtes vulnérables en quarantaine.

  - Créez des politiques manuelles dans des portées au sommet de votre arborescence ou à proximité de celui-ci.

    Par exemple, pour bloquer tout le trafic provenant de l'extérieur de votre réseau vers chaque hôte de votre réseau, placez la politique dans la portée en haut de l'arborescence.
  - Si vous souhaitez pouvoir remplacer la politique générale pour certaines charges de travail (par exemple, dans l'exemple ci-dessus, vous souhaitez bloquer l'accès général depuis l'extérieur de votre réseau, mais vous voulez que certaines charges de travail soient accessibles depuis l'extérieur de ce dernier), créez les politiques globales en tant que politiques par défaut. Créez ensuite des politiques spécifiques pour les charges de travail applicables.
  - Pensez à utiliser des modèles pour accélérer la création de politiques.
  - Consultez les sections Créer manuellement des politiques, à la page 441, Politiques à des fins précises, à la page 442 et Modèles de politiques, à la page 445.

- (Facultatif) Dans un premier temps, découvrez automatiquement les politiques d'une portée proche du sommet de votre arborescence, pour toutes les portées d'une branche de l'arborescence, afin de créer des politiques générales qui autorisent tout le trafic existant et limitent le futur trafic indésirable. Vous pouvez ensuite créer des politiques plus fines qui protègent votre réseau contre le trafic inutile ou indésirable.

  Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453 et Découvrir automatiquement les politiques, à la page 449 pour de plus amples renseignements.
- Lorsque vous êtes prêt à découvrir des politiques plus fines, découvrez automatiquement des politiques pour les portées situées au bas ou près du bas de l'arborescence de votre portée, en particulier dans les portées des applications individuelles.

  Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453 et Découvrir automatiquement les politiques, à la page 449 pour de plus amples renseignements.
- Assurez-vous d'avoir des politiques qui traitent des activités et des scénarios inhabituels ou rares, tels que le basculement, la restauration à partir d'une sauvegarde, les activités annuelles, etc.
- Après avoir identifié et autorisé le trafic nécessaire à vos applications, recherchez tout trafic qui ne devrait pas se produire et bloquez ces instances.

Examinez d'abord le trafic entrant et sortant de vos applications les plus sensibles.

Par exemple, si vous constatez du trafic depuis votre application Web destinée aux clients vers la base de données de votre application de recherche et développement top secrète, vous devez enquêter.

- Collaborez avec vos collègues pour vous assurer que les bonnes politiques sont appliquées aux bonnes charges de travail.
- Pour commencer, lorsque vous appliquez des politiques, envisagez de définir la règle collectrice sur Allow (autoriser). Ensuite, surveillez le trafic pour voir ce qui correspond à la règle collectrice. Lorsqu'aucun trafic nécessaire ne correspond à la règle « collectrice », vous pouvez définir ce paramètre sur Deny (Refuser).

Créer manuellement des politiques

En règle générale, vous pouvez créer manuellement des politiques qui s'appliquent globalement à votre réseau.

Par exemple, vous pouvez créer manuellement des politiques pour :

- Autoriser l'accès de toutes les charges de travail internes à vos serveurs NTP, DNS, Active Directory ou à l'analyse des vulnérabilités.
- Refuser l'accès de tous les hôtes extérieurs à votre organisation aux hôtes à l'intérieur de votre réseau, sauf autorisation explicite.
- Mettre les charges de travail vulnérables en quarantaine.

Vous pouvez créer des politiques absolues qui ne peuvent pas être remplacées par des politiques appliquées de manière plus granulaire, et des politiques par défaut qui peuvent être remplacées s'il existe une politique plus spécifique.

Vous pouvez créer des politiques manuelles pour les portées proches du sommet de votre arborescence.

Avant de commencer

- (Facultatif) Utilisez l'un des modèles disponibles à partir de **Defend (Défendre) – Policy Templates**(modèles de politique).
- (Facultatif) Si vous savez que vous possédez un ensemble de charges de travail qui reçoivent les mêmes politiques, utilisez un filtre d'inventaire pour les regrouper afin de pouvoir facilement appliquer des politiques à l'ensemble. Le filtre d'inventaire ne peut s'appliquer qu'à une seule portée ou à des charges de travail de n'importe quelle portée. Consultez Créer un filtre d'inventaire, à la page 392.
- Assurez-vous que les charges de travail de cette portée sont celles que vous prévoyez d'y trouver. Consultez Afficher les charges de travail d'une portée, à la page 432.

Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Dans la liste de gauche, recherchez ou accédez à la portée dans laquelle vous souhaitez créer la politique.

Étape 3 Cliquez sur la portée et l'espace de travail dans lesquels vous souhaitez créer la politique.

Si vous n'avez pas encore créé l'espace de travail pour cette portée, consultez Créer un espace de travail, à la page 431.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur l'onglet **Policies** (Politiques) s'il n'est pas déjà sélectionné.

Étape 6 Cliquez sur **Add Policy** (ajouter une politique).

Si vous ne voyez pas de bouton Add Policy (Ajouter une politique), consultez Si le bouton Add Policy (Ajouter une politique) n'est pas disponible, à la page 442.

Étape 7 Saisir des renseignements

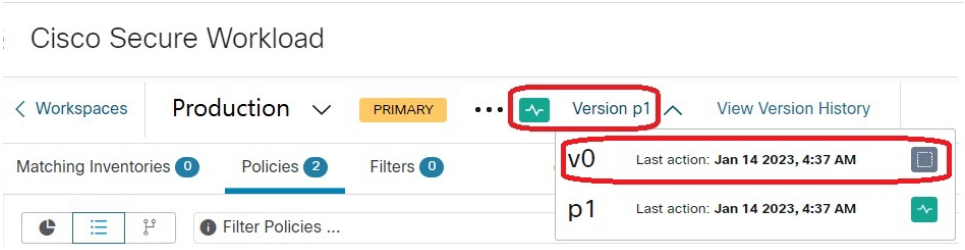
- Pour en savoir plus sur la case à cocher **Absolute** (Absolue), consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 437. En général, si vous créez des politiques pour lesquelles vous ne vous attendez pas à des exceptions, cochez cette case.
- **Priority (La priorité)** définit l'ordre de la politique dans la liste. Pour en savoir plus sur la définition de l'ordre des politiques, consultez Priorités des politiques, à la page 516 et les sous-sections. (Vous pouvez définir l'ordre des politiques ultérieurement).
- Le consommateur et le fournisseur peuvent correspondre à une portée entière ou, si vous avez créé des groupes de charges de travail à l'aide de filtres d'inventaire (ou, de manière moins optimale, des grappes dans le même espace de travail), vous pouvez les choisir.

Prochaine étape

Assurez-vous que l'action **Collectrice** est appropriée pour l'espace de travail. Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 437.

Si le bouton Add Policy (Ajouter une politique) n'est pas disponible

Si vous essayez de créer une politique et que le bouton **Add Policy** (ajouter une politique) n'est pas disponible, cliquez sur la version affichée en haut de la page et choisissez la dernière version « v », qui est indiquée par un carré gris :



Politiques à des fins précises

Créer des politiques InfoSec pour bloquer le trafic provenant de l'extérieur de votre réseau

Utilisez cette procédure pour créer rapidement un ensemble complet de politiques pour contrôler le trafic entrant dans votre réseau en provenance de l'extérieur. L'ensemble de règles par défaut autorise uniquement

le trafic utilisant des ports et des protocoles courants et refuse tout autre trafic. Vous pouvez modifier l'ensemble de règles par défaut selon vos besoins.

Avant de commencer

Utilisez cette procédure si les critères suivants sont remplis :

- Votre arborescence de portées a une portée nommée **Internal** (Interne) juste en dessous de la portée racine.

  Les membres de cette portée comprennent, ou incluront, des sous-réseaux englobant toutes les charges de travail sur votre réseau interne.

- La portée interne n'a encore aucune politique définie.

Remarque Sinon, vous pouvez utiliser le modèle **InfoSec** disponible dans **Defend > Policy Templates** (Défendre> Modèles de politiques) pour y parvenir en quelques étapes supplémentaires.

Procédure

Étape 1 Choisissez **Defend (défense) > Segmentation (segmentation).**

Étape 2 Cliquez sur la portée **Internal** (interne), puis sur l'espace de travail principal.

Si l'espace de travail principal n'existe pas encore, cliquez sur le bouton + pour le créer.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 Cliquez sur **Add InfoSec Policies** (Ajouter des politiques InfoSec).

Étape 5 Vérifiez que toutes les politiques de la liste, y compris les protocoles et les ports, sont des politiques que vous souhaitez, puis supprimez et modifiez les politiques comme à votre convenance.

Étape 6 Cliquez sur **Create** (créer).

Prochaine étape

(Facultatif) Ajoutez des politiques supplémentaires à votre portée interne, telles que les politiques qui autorisent certains trafics externes vers des charges de travail spécifiques.

Placez toutes les politiques spécifiques sous des politiques plus générales dans la liste.

Créer des politiques pour traiter les menaces immédiates

Si vous devez faire face à une menace immédiate, vous pouvez ajouter manuellement une politique absolue étroitement ciblée à une portée au sommet ou à proximité d ece dernier de votre arborescence, puis appliquer l'espace de travail principal à cette portée.

Après avoir corrigé la menace, vous pouvez supprimer cette politique et renforcer l'espace de travail.

Créer une politique de mise en quarantaine des charges de travail vulnérables

Vous pouvez réaliser les actions suivantes :

- Créer des politiques à l'avance pour mettre automatiquement en quarantaine les charges de travail présentant des vulnérabilités connues ou un seuil de gravité de vulnérabilité que vous définissez.
- Créer des politiques pour mettre immédiatement en quarantaine les charges de travail pour lesquelles des vulnérabilités connues ont été détectées et que vous jugez suffisamment problématiques.

Cette rubrique décrit le processus à suivre dans les deux cas.

Avant de commencer

Examinez Afficher le tableau de bord des vulnérabilités, à la page 861 pour voir quelles politiques sont requises.

Procédure

Étape 1 Créez un filtre d'inventaire qui définit les vulnérabilités ou le seuil de gravité de la vulnérabilité que vous souhaitez mettre en quarantaine :

a) Dans la barre de navigation à gauche de la fenêtre, choisissez **Organiser > Filtres d'inventaire** (Organiser > Filtres d'inventaires).
b) Cliquez sur **Create Inventory Filter (créer un filtre d'inventaire).**
c) Cliquez sur le bouton **(i)** à côté de **Query** (requête) et saisissez `CVE` pour afficher les options de filtre appropriées.
d) Saisissez les critères de filtre qui déterminent les charges de travail que vous souhaitez mettre en quarantaine.
e) Assurez-vous que l'option **Restrict query to ownership scope** (Restreindre la requête à la portée de la propriété) n'est PAS cochée.

Étape 2 Créez une politique pour mettre en quarantaine les charges de travail touchées :

Pour plus d'informations générales sur les instructions, consultez Créer manuellement des politiques, à la page 441.

les recommandations :

- Créez la politique dans votre portée **interne** ou autre près du sommet de votre arborescence.
- La politique doit être une politique absolue, sauf si vous souhaitez autoriser des exceptions. Assurez-vous de créer des politiques pour traiter d'éventuelles exceptions.
- Créez des politiques distinctes pour le consommateur et le fournisseur.
- Définissez la priorité de chaque politique sur un nombre faible afin qu'elle soit atteinte avant les autres politiques de la liste.
- Définissez l'action sur **Deny** (Refuser).

Étape 3 Examiner, analyser et appliquer la politique ou les politiques.

Prochaine étape

Créez une alerte pour être averti lorsque le trafic atteint cette politique afin de pouvoir résoudre le problème et restaurer le trafic vers la charge de travail vulnérable. Consultez Configurer les alertes, à la page 673.

Modèles de politiques

Les modèles de politiques sont utilisés pour appliquer des ensembles de politiques similaires à plusieurs espaces de travail.

Cisco Secure Workload comprend des modèles prédéfinis, et vous pouvez créer vos propres modèles.

Les modèles de politique nécessitent la capacité de propriétaire de la portée sur la portée racine.

Modèles de politiques définis par le système

Pour afficher les modèles de politique disponibles, accédez à **Defend > Policy Templates** (Défendre > Modèles de politique).

Pour utiliser un modèle de politique, consultez Application d'un modèle, à la page 448.

Pour modifier un modèle défini par le système, téléchargez le fichier JSON, modifiez-le, puis téléversez-le.

Créer des modèles de politiques personnalisés

Schéma JSON pour les modèles de politique

Le schéma JSON du modèle de politique est conçu pour imiter le schéma des Exporter un espace de travail. Vous pouvez créer un ensemble de politiques dans un espace de travail, l'exporter au format JSON, modifier le JSON, puis l'importer en tant que modèle de politique.

Attribut	Type	Description
name	chaîne	(Facultatif) Utilisé comme nom du modèle lors de l'importation.
description	chaîne	(Facultatif) Description du modèle qui s'affiche pendant le processus d'application.
paramètres	objet Paramètres	Paramètres du modèle, voir ci-dessous.
absolute_policies	tableau d'objets politiques	(Facultatif) Tableau de politiques absolues.
default_policies	tableau d'objets politiques	(obligatoire) Le tableau de politiques par défaut peut être vide.

Objet Paramètres

L'objet Paramètres est facultatif, mais il peut être utilisé pour définir dynamiquement des filtres en tant que paramètres du modèle. Les paramètres sont référencés à l'aide des attributs de politique `consumer_filter_ref` ou `provider_filter_ref`.

Les clés de l'objet Paramètres sont les noms de référence. Les valeurs sont un objet avec un « `type` » obligatoire. « `Filter` » et une description facultative. Un exemple d'objet Paramètres est présenté ci-dessous :

```
{
```

```
  "parameters": {
    "HTTP Consumer": {
      "type": "Filter",
      "description": "Consumer of the HTTP and HTTPS service"
    },
    "HTTP Provider": {
      "type": "Filter",
      "description": "Provider of the HTTP and HTTPS service"
    }
  }
}
```

Les paramètres peuvent être référencés dans les objets de politique, par exemple : « consumer_filter_ref » : « HTTP Consumer » ou « provider_filter_ref » : « HTTP Provider ».

Références de paramètres spéciaux

Quelques références particulières sont automatiquement mappées à un filtre et n'ont pas besoin d'être définies comme paramètres.

Référence	Description
_workspaceScope	Détermine la portée de l'espace de travail auquel le modèle est appliqué.
_rootScope	Résout la portée de niveau racine/supérieur.

Objet politique

Pour maintenir la compatibilité avec le JSON d'exportation d'espace de travail, l'objet politique contient plusieurs clés pour les consommateurs et les fournisseurs. Ces objets sont résolus comme suit :

```
if *_filter_ref is defined
  use the filter resolved by that parameter
else if *_filter_id is defined
  use the filter referenced by that id
else if *_filter_name is defined
  use the filter that has that name
else
  use the workspace scope.
```

Si un filtre ne peut pas être résolu comme défini ci-dessus, une erreur est renvoyée au moment de l'application et au moment du téléchargement.

Attribut	Type	Description
action	chaîne	(facultatif) Action de la politique, ALLOW (AUTORISER)ou DENY (REFUSER)(ALLOW par défaut).
priority	nombre entier	(Facultatif) Priorité de la politique (100 par défaut).
consumer_filter_ref	chaîne	Référence à un paramètre.
consumer_filter_name	chaîne	Référence à un filtre par nom.

Attribut	Type	Description
consumer_filter_id	chaîne	l'identifiant d'une portée ou d'un filtre d'inventaire défini.
provider_filter_ref	chaîne	Référence à un paramètre.
provider_filter_name	chaîne	Référence à un filtre par nom.
provider_filter_id	chaîne	l'identifiant d'une portée ou d'un filtre d'inventaire défini.
l4_params	tableau de l4params	Liste des ports et des protocoles autorisés.
Attribut	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	nombre entier	Plage de ports inclusive, par exemple, [80, 80] ou [5000, 6000] (NULL signifie tous les ports).

Objet L4param

Attribut	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	nombre entier	Plage de ports inclusive, par exemple, [80, 80] ou [5000, 6000] (NULL signifie tous les ports).

Échantillon de modèle

```
{
  "name": "Allow HTTP/HTTPS and SSH",
  "parameters": {
    "HTTP Consumer": {
      "type": "Filter",
      "description": "Consumer of the HTTP and HTTPS service"
    },
    "HTTP Provider": {
      "type": "Filter",
      "description": "Provider of the HTTP and HTTPS service"
    }
  },
  "default_policies": [
    {
      "action": "ALLOW",
      "priority": 100,
      "consumer_filter_ref": "__rootScope",
      "provider_filter_ref": "__workspaceScope",
      "l4_params": [
```

```
        { "proto": 6, "port": [22, 22] },
      ]
    },
    {
      "action": "ALLOW",
      "priority": 100,
      "consumer_filter_ref": "HTTP Consumer",
      "provider_filter_ref": "HTTP Provider",
      "l4_params": [
        { "proto": 6, "port": [80, 80] },
        { "proto": 6, "port": [443, 443] }
      ]
    }
  ]
}
```

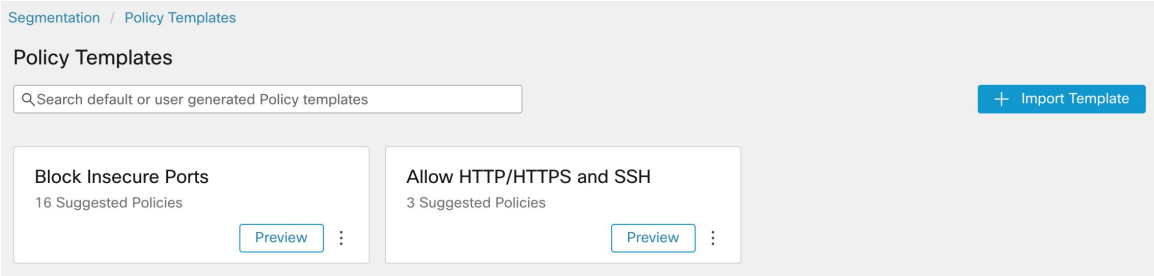
Importation de modèle

Les modèles de politiques sont affichés dans la page des modèles de politiques et accessibles à partir de la page principale de segmentation. C'est à ce niveau que les modèles peuvent être importés ou téléchargés en utilisant le bouton « Import Template) Importer un modèle ».

L'exactitude des modèles est validée lorsqu'ils sont téléversés. Une liste d'erreurs utile est fournie pour déboguer les problèmes.

Une fois qu'un modèle est téléversé, le nom et la description peuvent être appliqués, téléchargés ou mis à jour.

Figure 249: Affichage des modèles disponibles



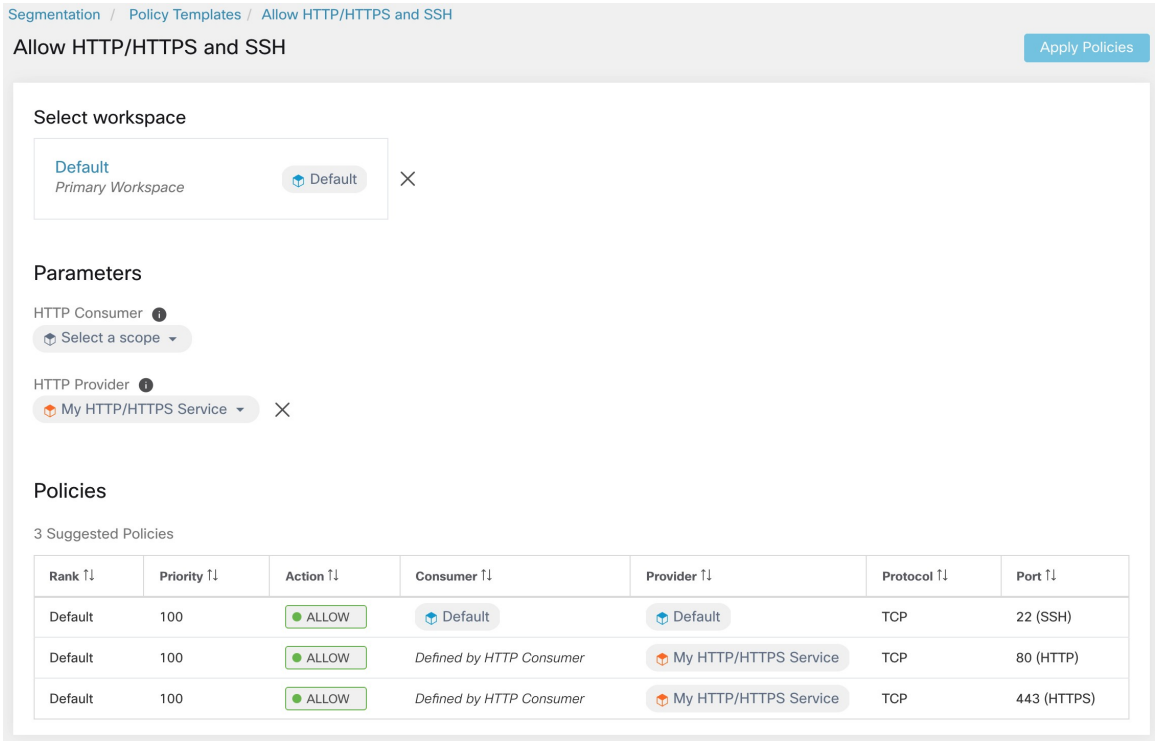
Application d'un modèle

L'application d'un modèle à un espace de travail se fait en plusieurs étapes :

1. Sélectionnez un modèle pour obtenir un aperçu.
2. Sélectionnez un espace de travail auquel appliquer le modèle.
3. Renseignez les paramètres si nécessaire.
4. Passez en revue les politiques.
5. Appliquez les politiques.

Les politiques seront ajoutées à la dernière version de l'espace de travail sélectionné. Les politiques créées à l'aide d'un modèle peuvent être filtrées à l'aide de l`From Template? (Du modèle?) = vrai` pour le filtre.

Figure 250: Application d'un modèle de politique



Découvrir automatiquement les politiques

La découverte automatique des politiques, parfois appelée détection de politiques et anciennement ADM (Application Dependency Mapping), utilise les flux de trafic existants et d'autres données pour effectuer ce qui suit :

- Suggérer un ensemble de politiques « autorisées » en fonction de l'activité réussie du réseau.

  L'objectif de ces politiques est d'identifier le trafic dont votre entreprise a besoin et de bloquer tout autre trafic.

- Regrouper les charges de travail en grappes en fonction de la ressemblance de leur comportement informatique

  Par exemple, si une application comprend plusieurs serveurs Web, ceux-ci peuvent être regroupés.

  Pour en savoir plus, consultez Grappes, on page 506.

Vous pouvez découvrir des politiques pour chaque portée. En règle générale, vous découvrez les politiques pour les portées au bas de l'arborescence ou près de celle-ci, par exemple au niveau de l'application. Cependant, pour le déploiement initial, vous pouvez souhaiter découvrir les politiques à une portée de niveau supérieur, de sorte que vous avez des politiques générales temporaires en place pendant que vous créez des politiques plus affinées.

Vous pouvez procéder à la découverte des politiques aussi souvent que vous le souhaitez pour affiner les suggestions de politiques en fonction d'informations supplémentaires.

Vous pouvez modifier manuellement les politiques et les grappes suggérées, et/ou les approuver, afin qu'elles soient reportées et non modifiées par les cycles de découverte ultérieurs.

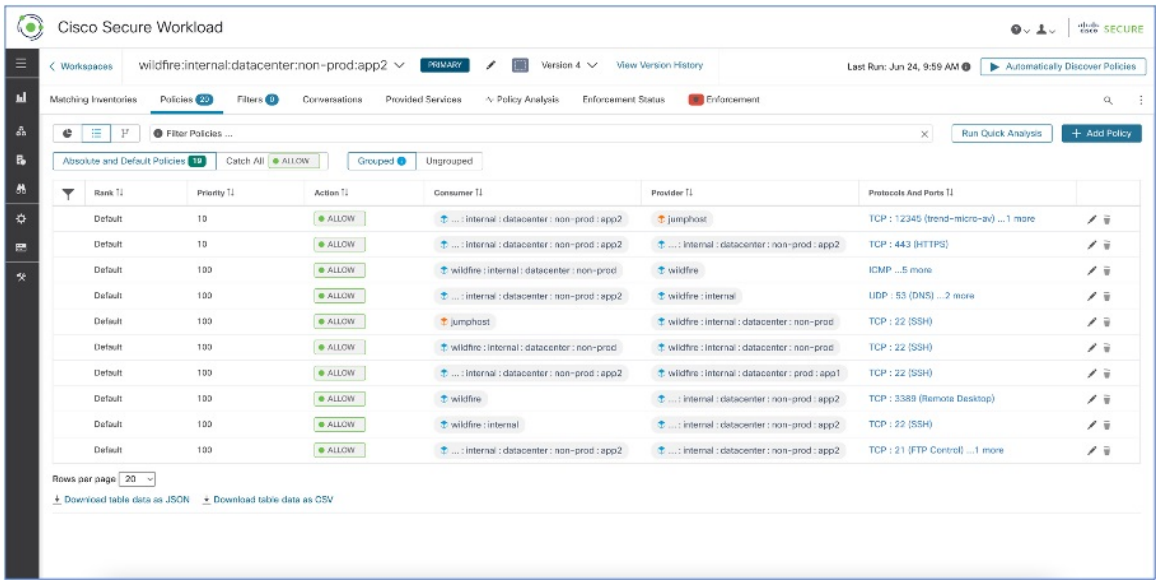
Vous pouvez inclure les politiques créées manuellement et les politiques découvertes dans un espace de travail.

Après avoir découvert les politiques, vous les passerez en revue et les analyserez avant de les appliquer.

Pour commencer à découvrir les politiques, consultez Comment découvrir automatiquement les politiques, on page 451.

Pour en savoir plus, consultez Détails de la découverte des politiques, on page 450.

Figure 251: Exemple : politiques détectées automatiquement



Détails de la découverte des politiques

Renseignements supplémentaires sur la découverte automatique des politiques :

- La découverte automatique des politiques prend en compte les conversations dans lesquelles au moins une extrémité est une charge de travail de membre de la portée dans la plage temporelle sélectionnée. L'appartenance à la portée est basée uniquement sur la définition la plus récente de la portée; l'appartenance antérieure n'est pas prise en compte.
- Par défaut, la découverte de politiques produit des politiques et des grappes en analysant les flux de communication (« conversations »), mais peut éventuellement prendre en compte d'autres renseignements tels que les processus en cours d'exécution sur les charges de travail ou les configurations d'équilibreurs de charge.

  Consultez Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques, à la page 467.
- Vous pouvez découvrir des politiques dans n'importe quel espace de travail de la portée. Les résultats de la découverte de chaque espace de travail sont indépendants des résultats des autres espaces de travail de la portée.

- Pour lire les des discussions détaillées sur les concepts complexes liés à la découverte automatique des politiques, consultez Fonctionnalités avancées de découverte automatique des politiques, à la page 459 et Aborder les complexités de la politique, à la page 515.

Comment découvrir automatiquement les politiques

Effectuez les étapes suivantes. À tout moment, vous pouvez décider de découvrir à nouveau les politiques.

Collaborez avec des collègues, au besoin, pour effectuer ces étapes.

Étape	Faire ceci	Autres renseignements
1	Chargez et étiquetez votre inventaire de charge de travail, et recueillez les données de flux qui informent la découverte des politiques.	Consultez Premiers pas avec la segmentation et la microsegmentation, à la page 2 et les sous-sections.
2	Choisissez si vous souhaitez découvrir les politiques pour : • Les charges de travail dans une seule portée • Les charges de travail dans toutes les portées d'une branche de l'arborescence des portées	Consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453. (Vous pouvez toujours redécouvrir les politiques à tout moment).
3	Choisissez la portée dans laquelle vous découvrez les politiques.	Cela dépend en partie du fait que vous découvriez des politiques pour une seule portée ou pour une branche de l'arborescence des portées.
4	Choisissez l'espace de travail dans lequel vous découvrez les politiques.	En général, vous découvrirez les politiques dans l'espace de travail principal de la portée, car vous ne pouvez analyser les politiques que dans un espace de travail principal. (Cependant, vous pouvez toujours remplacer un espace de travail par un principal ultérieurement). Si le portée que vous avez choisi ne comporte pas encore d'espace de travail, consultez Créer un espace de travail, à la page 431.
5	Confirmez l'inventaire que vous souhaitez inclure dans la découverte de politiques.	Vérifier les charges de travail auxquelles la découverte de politiques s'appliquera, à la page 455
6	(Facultatif) Créez des filtres d'inventaire pour regrouper les charges de travail que vous souhaitez traiter comme un groupe.	Consultez Créer un filtre d'inventaire, à la page 392.
7	Définissez l'action **Collectrice** (c'est à dire fourre-tout) pour l'espace de travail	Voir la section Rang de politique : Absolue, Par défaut et Collectrice, à la page 437.

Étape	Faire ceci	Autres renseignements
8	Découvrir les politiques	Découvrir automatiquement les politiques, à la page 449 Assurez-vous de remplir les conditions préalables décrites dans la section « Avant de commencer ».
9	Afficher et gérer les grappes (groupes de charges de travail) créées par la découverte de politiques. (Cette étape s'applique uniquement lorsque vous découvrez des politiques pour une seule portée; les grappes ne sont pas générées lorsque vous découvrez des politiques pour une branche de l'arborescence).	Consultez Grappes, à la page 506 et les sous-sections. Évaluez les grappes suggérées, modifiez éventuellement l'appartenance aux grappes le cas échéant et approuvez (ou mieux encore, convertissez en filtres d'inventaire) toutes les grappes que vous souhaitez rendre permanentes.
10	Tenez compte des complexités telles que l'hérédité des politiques et les politiques multiportées.	Consultez Aborder les complexités de la politique, à la page 515.
11	Examiner les politiques générées.	Consultez Consulter les politiques découvertes automatiquement, à la page 538 et les sous-sections.
12	Approuvez les politiques que vous souhaitez conserver.	Approuver les politiques, à la page 479
13	Découvrez à nouveau les politiques si vous le souhaitez, pour refléter des données de flux supplémentaires, des changements dans la composition de la portée, ou d'autres changements.	Important : Avant de réexécuter la découverte automatique des politiques, à la page 482 Vous pouvez réexécuter la découverte de politiques à tout moment. Passez en revue et approuvez les politiques et les groupes chaque fois que vous découvrez des politiques.
14	Exécutez une analyse en direct pour voir comment vos politiques affectent votre trafic réel.	Lorsque vous estimez que vos politiques produisent ce que vous attendez d'elles, démarrez Analyse des politiques en temps réel, à la page 546. Si vous modifiez les politiques ou les redécouvrez, redémarrez l'analyse des politiques (pour analyser les politiques actuelles).
15	Si vous redécouvrez des politiques ou apportez d'autres modifications, redémarrez l'analyse en direct.	Consultez Après avoir modifié les politiques, analyser les dernières politiques, à la page 555.
16	Lorsque vous êtes sûr que les politiques ne bloqueront pas le trafic essentiel, appliquez l'espace de travail.	Voir Appliquer des politiques et les sous-thèmes.
17	Vérifier que l'application fonctionne comme prévu.	Voir la section Vérifier que l'application fonctionne comme prévu, à la page 567.

Étape	Faire ceci	Autres renseignements
18	(Facultatif) Configurez les paramètres de découverte de politiques par défaut qui s'appliquent facultativement lors de la découverte de politiques dans n'importe quel espace de travail.	Consultez Configuration de la découverte de politiques par défaut, à la page 477 et les rubriques connexes. Puisqu'il s'agit de paramètres avancés, nous vous recommandons de les modifier uniquement si vous avez un besoin particulier de le faire. Vous pouvez les modifier à tout moment au cours de votre processus si vous prenez conscience d'un besoin.

Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée

Si l'une ou l'autre de ces options n'est possible lorsque vous découvrez les politiques pour une portée particulière, la sélection est effectuée pour vous, et vous ne verrez pas de choix d'options.

Tableau 24 : Découverte des politiques pour :

Une branche de l'arborescence de la portée	Une seule portée
Utilisez cette méthode comme point de départ, lorsque vous commencez à utiliser Cisco Secure Workload, pour générer rapidement un ensemble temporaire de politiques générales qui autorisent le trafic existant tout en vous aidant à protéger votre réseau contre les menaces futures.	Utilisez cette méthode pour affiner les politiques de segmentation et vous assurer que tous les flux autorisés sont attendus; le nombre plus restreint de politiques permet de repérer plus facilement les anomalies existantes qui nécessitent une enquête.
En règle générale, vous utilisez cette méthode pour les portées situées plus près du sommet de votre arborescence. Le sommet de la branche peut correspondre à n'importe quelle portée dans l'arborescence.	En règle générale, vous utilisez cette méthode pour les portées situées au bas de l'arborescence, par exemple pour les portées dédiées à une seule application.
Politiques de découverte uniquement dans une seule portée : la portée située en haut de la branche de votre choix.	Découvrir les politiques pour chaque portée de la branche, le cas échéant.
Toutes les charges de travail dans la portée choisie et toutes les portées enfants et descendants sont incluses dans la découverte.	Les charges de travail qui sont également membres d'une portée enfant ne sont pas incluses dans la découverte pour cette portée. Les politiques sont générées uniquement pour les charges de travail qui apparaissent dans l'onglet **Uncategorized Inventory (Inventaire non classé)** pour cette portée sur la page **Organize > Scopes and Inventory** (Organiser > Portées et inventaire). Vous pouvez découvrir des politiques pour les charges de travail dans les portées enfant et descendante séparément.

Une branche de l'arborescence de la portée	Une seule portée
Toutes les politiques relatives aux charges de travail de toutes les portées de la branche résident dans la portée située au sommet de la branche.	En supposant que vous créiez également des politiques pour les charges de travail dans les portées enfant et descendante, les politiques résident dans plusieurs portées.
Cette méthode génère généralement un grand nombre de politiques.	Cette méthode génère moins de politiques dans une portée individuelle.
Les politiques découvertes s'appliquent à des portées entières; cette option ne peut pas créer de politiques propres aux sous-ensembles de charges de travail dans les portées.	Cette option peut générer des politiques qui s'appliquent à des sous-ensembles de charges de travail dans la portée du consommateur ou du fournisseur. (Les charges de travail peuvent être regroupées par grappes générées ou par filtres d'inventaire configurés, et les politiques appliquées uniquement à ces sous-ensembles).
Toutes les politiques sont créées dans une seule portée, en haut de la branche, donc aucune étape supplémentaire n'est requise lorsque le consommateur et le fournisseur d'une politique se trouvent dans des portées différentes.	Autoriser le trafic entre les consommateurs et les fournisseurs dans différentes portées nécessite des étapes supplémentaires. Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 522.
La découverte peut s'exécuter même si une portée n'a aucune charge de travail de membre avec des agents installés, tant que les portées descendantes comportent des agents ou des orchestrateurs ou des connecteurs externes qui recueillent les données de flux.	La portée doit avoir des charges de travail de membres avec des agents installés ou des orchestrateurs ou des connecteurs externes qui recueillent des données de flux.
Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site.	Vous devez avoir des privilèges pour créer des politiques pour cette portée.
Le nombre maximal d'agents et de conversations est différent pour chaque option. Consultez Limites liées aux politiques, à la page 1172.	
Cette option était auparavant l'option de configuration avancée Advanced Policy Generation pour la découverte automatique des politiques. Le comportement n'a pas changé.	Il s'agissait auparavant du comportement par défaut pour la découverte automatique des politiques.
Pour en savoir plus, consultez Découverte des politiques pour une branche de l'arborescence d'une portée : informations supplémentaires, à la page 454.	--

Découverte des politiques pour une branche de l'arborescence d'une portée : informations supplémentaires

- Toutes les charges de travail qui sont des points terminaux de conversation, qu'elles soient membres ou non de la portée dans laquelle la découverte de politiques est exécutée, reçoivent l'étiquette de portée correspondante la plus élevée en fonction de l'ordre ascendant donné dans la liste des dépendances externes.

- Pour les options de configuration avancée disponibles lorsque vous générez des politiques pour une branche de l'arborescence de portée, consultez :
  - Activer la suppression des politiques redondantes, à la page 474
  - Compression des politiques, à la page 470 et les sous-thèmes connexes, Compression hiérarchique des politiques, à la page 470
- Actuellement, le nombre de charges de travail affiché pour la découverte automatique des politiques n'inclut que celles qui ne sont pas également membres d'une sous-portée.

Vérifier les charges de travail auxquelles la découverte de politiques s'appliquera

Avant de découvrir automatiquement les politiques, vérifiez que les charges de travail sur lesquelles la découverte de politiques sera basée correspondent bien à l'ensemble de charges de travail attendu. Les politiques de découvertes seront générées à partir des données de flux capturées par les agents sur ces charges de travail.

Avant de commencer

Décidez laquelle des options de Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453 vous pouvez utiliser.

Procédure

Étape 1 Dans le menu de navigation de gauche, choisissez **Defend > Segmentation**(défense > segmentation).

Étape 2 Cliquez sur la portée pour laquelle vous souhaitez découvrir les politiques.

Étape 3 Cliquez sur l'espace de travail dans lequel vous souhaitez découvrir les politiques.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur **Matching Inventories** (Inventaires correspondants).

Étape 6 Si vous découvrez des politiques pour une seule portée :

a) Cliquez sur **Uncategorized Inventory** (Inventaire non classé)

Cette page affiche les charges de travail qui ne sont pas également membres des portées enfants. (Dans la découverte automatique des politiques standard, les politiques et les grappes sont générées dans cette portée uniquement pour les charges de travail qui ne sont pas également membres des portées enfants).

b) Cliquez sur **IP Addresses** (Adresses IP).

Les adresses IP sur cette page ne comportent pas d'agents Cisco Secure Workload.

Puisqu'elles n'ont pas d'agents installés, ces adresses IP ne sont pas prises en compte lors de la découverte automatique des politiques pour cette portée sauf dans les cas suivants :

- La politique est gérée par un connecteur infonuagique
- Les adresses IP sont basées sur un inventaire fondé sur le conteneur, auquel cas les charges de travail individuelles apparaissent sur l'onglet « **Pods** », ou
- les charges de travail communiquent avec une charge de travail dans cette portée prise en compte lors de la découverte de politique.

Avant de découvrir les politiques, envisagez d'installer des agents sur les charges de travail qui en ont besoin et de laisser passer un certain temps pour que les données de flux s'accumulent.

c) Cliquez sur **Workloads** (Charges de travail).

Les politiques et les grappes sont générées uniquement pour les charges de travail sur cette page et pour les adresses IP dans l'onglet IP address (adresses IP) qui répondent aux critères précisés ci-dessus.

d) Si vous avez un inventaire Kubernetes ou OpenShift, vous verrez un onglet **Services** et un onglet **Pods**.

Si vous avez installé des agents sur vos charges de travail Kubernetes/OpenShift vérifiez également l'inventaire dans ces onglets.

e) Si vous avez un inventaire de l'équilibreur de charge, celui-ci s'affiche sous l'onglet **Services**.

Étape 7 Si vous découvrez des politiques pour une branche de l'arborescence :

a) Cliquez sur **All Inventory** (Tout l'inventaire).

Ce processus génère des politiques (mais pas de grappes) pour toutes les charges de travail de cette portée, qu'elles soient également membres ou non de portées enfants.

b) Cliquez sur **IP Addresses** (Adresses IP).

Les adresses IP sur cette page ne comportent pas d'agents Cisco Secure Workload.

Puisqu'aucun agent n'est installé, ces adresses IP ne seront pas prises en compte lors de la découverte automatique des politiques pour cette portée, sauf si :

- La politique est gérée par un connecteur infonuagique
- Les adresses IP sont basées sur un inventaire fondé sur le conteneur, auquel cas les charges de travail individuelles apparaissent sur l'onglet « **Pods** », ou
- les charges de travail communiquent avec une charge de travail dans cette portée prise en compte lors de la découverte de politique.

Avant de découvrir les politiques, pensez à installer des agents sur ces charges de travail et attendez que les données de flux s'accumulent.

c) Cliquez sur **Workloads** (Charges de travail).

Les politiques sont générées uniquement pour les charges de travail sur cette page et pour les adresses IP dans l'onglet IP address (adresses IP) qui répondent aux critères précisés ci-dessus.

d) Si vous avez un inventaire Kubernetes ou OpenShift, vous verrez un onglet **Services** et un onglet **Pods**.

Si vous avez installé des agents sur vos charges de travail Kubernetes/OpenShift vérifiez également l'inventaire dans ces onglets.

e) Si vous avez un inventaire de l'équilibreur de charge, celui-ci s'affiche sous l'onglet **Services**.

Étape 8 Vérifiez que les charges de travail sont bien l'ensemble attendu.

Découvrir automatiquement les politiques

Utilisez cette procédure pour générer des suggestions de politiques d'autorisation en fonction du trafic existant sur votre réseau.

Vous pouvez réexécuter la découverte de politiques à tout moment.

Avant de commencer

- Rassembler des données de flux avant de pouvoir découvrir automatiquement les politiques.

  En général, cela signifie que vous avez installé les agents sur les charges de travail de la portée, ou que vous avez configuré et recueilli des données à l'aide d'un connecteur infonuagique ou d'un orchestrateur externe.

  Les données de résumé de flux utilisées par la découverte automatique des politiques sont calculées toutes les 6 heures. Ainsi, lors du déploiement initial de Cisco Secure Workload, la découverte automatique des politiques n'est pas possible tant que ces données ne sont pas disponibles.

  Un plus grand nombre de données de flux produit généralement des résultats plus précis.

  Avant d'appliquer une politique, vous devez recueillir suffisamment de données pour inclure le trafic qui ne se produit que périodiquement (mensuel, trimestriel, annuel, etc.). Par exemple, si une application génère un rapport trimestriel qui recueille des informations provenant de sources auxquelles l'application n'accède pas à d'autres moments, assurez-vous que les données de flux incluent au moins une instance de ce processus de génération de rapports.

- Suivez les étapes décrites ci-dessus dans Comment découvrir automatiquement les politiques, à la page 451.
- Respectez le Limites liées aux politiques, à la page 1172 liée à la découverte des politiques

  Si nécessaire, scindez les portées les plus importantes en portées enfants plus petites.

- Validez toutes les modifications de portée avant de découvrir les politiques, sinon les filtres d'exclusion configurés pourraient ne pas correspondre aux flux comme prévu (ne pas les exclure). Consultez Valider les modifications, à la page 377.

Important Si vous réexécutez la découverte de politiques, consultez d'abord ces considérations importantes : Important : Avant de réexécuter la découverte automatique des politiques, à la page 482.

Procédure

Étape 1 Sélectionnez**Defend (Défendre)** > **Segmentation (Segmentation)**.

Étape 2 Dans l'arborescence des portées ou dans la liste des portées dans le volet de gauche, faites défiler la liste ou recherchez la portée pour laquelle vous souhaitez générer des politiques.

Étape 3 Cliquez sur un espace de travail (principal ou secondaire) dans la portée.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 5 Cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques).

Étape 6 Si vous voyez une option pour découvrir des politiques dans une branche de l'arborescence ou une portée complète, choisissez une option.

Si vous ne voyez pas d'option, une seule option est possible pour la portée pour laquelle vous découvrez des politiques.

Pour en savoir plus, consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, à la page 453.

Étape 7 Choisissez la plage temporelle des données de flux que vous souhaitez inclure.

Testez pour déterminer la bonne plage temporelle; vous pouvez générer des politiques aussi souvent que nécessaire pour obtenir des résultats optimaux.

Une plage temporelle plus courte génère des résultats plus rapidement et peut en générer moins.

En général, une plage temporelle plus longue produit des politiques plus précises. Toutefois, si la définition de la portée a été modifiée, n'incluez pas les dates précédant la modification.

Votre plage temporelle doit inclure le trafic qui ne se produit que périodiquement (mensuel, trimestriel, annuel, etc)., le cas échéant. Par exemple, si une application génère un rapport trimestriel qui recueille des renseignements provenant de sources auxquelles elle n'accède pas à d'autres moments, assurez-vous que la plage temporelle comprend au moins une instance de ce processus de génération de rapports.

Pour configurer une plage temporelle au-delà des 30 derniers jours, sélectionnez la plage **personnalisée** et remplissez les heures de début et de fin requises dans le gadget déroulant de sélection de l'heure.

Étape 8 (Facultatif) Spécifiez les paramètres avancés.

En général, nous vous suggérons de ne pas modifier les paramètres avancés des cycles de découverte initiaux, puis d'apporter les modifications nécessaires uniquement pour la résolution de problèmes spécifiques.

Pour de plus amples renseignements, consultez la section Configurations avancées pour la découverte automatique des politiques, à la page 467.

Étape 9 Cliquez sur **Discover Policies** (Découvrir les politiques). Les politiques générées s'affichent sur cette page.

Prochaine étape

- Affichez Arrêter la découverte automatique des politiques en cours, à la page 458.
- Revenez à Comment découvrir automatiquement les politiques, à la page 451 et passez à l'étape suivante dans le tableau.
- Vous pouvez réexécuter la découverte de politiques à tout moment. Pour connaître les actions à effectuer en premier, consultez Important : Avant de réexécuter la découverte automatique des politiques, à la page 482.

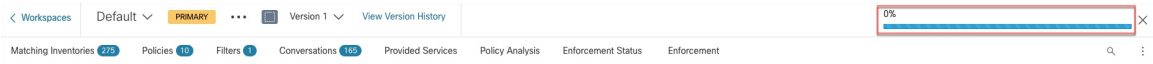
Arrêter la découverte automatique des politiques en cours

La progression de la découverte automatique des politiques est toujours visible dans l'en-tête. La navigation vers d'autres espaces de travail n'affecte pas la progression.

Pour arrêter l'analyse pendant qu'elle est en cours, cliquez sur le bouton **Abort** (abandonner).

Une fois l'analyse terminée, un message s'affiche. En cas de réussite, **Cliquez pour voir les résultats** permet d'accéder à une vue différente indiquant les modifications avant et après l'exécution. L'échec de la découverte automatique des politiques est indiqué par un message et une raison différents.

Figure 252: Progression de la découverte automatique des politiques



Fonctionnalités avancées de découverte automatique des politiques

Vous devez spécifier une plage temporelle pour l'exécution de la découverte. Au besoin, vous pouvez configurer des options avancées.

Vous pouvez configurer des options avancées pour chaque espace de travail ou définir des valeurs par défaut pour tous les espaces de travail (l'ensemble de la portée racine), puis modifier les paramètres de chaque espace de travail au besoin.

Tableau 25 : Configurer les options avancées pour la découverte automatique des politiques

Pour un espace de travail	Pour tous les espaces de travail
Les descriptions des options pour les espaces de travail individuels (dans la colonne 1) s'appliquent également à tous les espaces de travail (dans la colonne 2).	
Dépendances externes, à la page 462	Configuration de la découverte de politiques par défaut, à la page 477
Configurations avancées pour la découverte automatique des politiques, à la page 467	Configuration de la découverte de politiques par défaut, à la page 477
Filtres d'exclusion, à la page 459	Filtres d'exclusion par défaut, à la page 478

Filtres d'exclusion

Si certains flux génèrent des politiques indésirables, vous pouvez exclure ces flux de la découverte automatique des politiques à l'aide de filtres d'exclusion.

Par exemple, pour interdire certains protocoles comme ICMP dans le modèle de liste d'autorisation finale, vous pouvez créer un filtre d'exclusion avec un champ de protocole défini à ICMP.

Note

- Les conversations qui correspondent aux filtres d'exclusion sont exclues à des fins de génération de politiques et de mise en grappe, mais restent présentent dans l'affichage des conversations avec l'icône rouge « excluded » (exclue) (voir la vue du tableau dans Conversations). De même, les charges de travail de l'espace de travail impliquées dans ces conversations restent également visibles.
- Un filtre d'exclusion qui utilise une grappe ou une définition de filtre d'un espace de travail n'est efficace que dans les espaces de travail principaux (sinon, ses définitions de grappe ne sont pas visibles par le système d'étiquettes et toutes les conversations correspondantes ne sont pas exclues).
- Les filtres d'exclusion font l'objet de versions; pour suivre les modifications, consultez Journaux d'activités et historique des versions (Historique et Diff.).
- Pour connaître les limites du nombre de filtres d'exclusion, consultez Limites liées aux politiques, on page 1172.

Vous pouvez créer l'un des éléments suivants ou les deux, puis activer l'un ou l'autre ou les deux lors de la découverte des politiques :

- Une liste de filtres d'exclusion pour chaque espace de travail.
- Une liste de filtres d'exclusion par défaut disponibles pour tous les espaces de travail de votre détenteur.

Vous pouvez également activer ou désactiver l'une des listes ou les deux pour la configuration de découverte de politiques par défaut.

Pour plus de renseignements sur les instructions, consultez Configurer, modifier ou supprimer les filtres d'exclusion, on page 460 et Activer ou désactiver les filtres d'exclusion, on page 462.

Configurer, modifier ou supprimer les filtres d'exclusion

Vous pouvez utiliser cette procédure pour créer une liste de filtres d'exclusion pour un espace de travail unique, ou une liste de filtres d'exclusion par défaut qui sont disponibles pour tous les espaces de travail.

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

Destinataire	Faire ceci
Configurer les filtres d'exclusion pour un espace de travail spécifique	Accédez à l'espace de travail, puis effectuez l'une des opérations suivantes : • Cliquez sur **Manage Policies**(gestion des politiques), puis sur le (Autre) près du coin supérieur droit de la page et sélectionnez **Exclusion Filters** (filtres d'exclusion). • Dans la page de configuration de découverte automatique des politiques, cliquez sur le lien **Exclusion Filters** (Filtres d'exclusion) dans la section Advanced Configurations (Advanced Configurations). • Supprimer une politique découverte; vous verrez une option pour créer un filtre d'exclusion qui le permette.
Configurer les filtres d'exclusion par défaut qui sont disponibles pour n'importe quel espace de travail	1. Choisissez **Defend (défense)** > **Segmentation (segmentation**, 2. Cliquez sur le signe d'insertion sur le côté droit de la page pour développer le menu Outils, puis choisissez **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut). 3. Accédez au bas de la page 4. Cliquez sur **Default Exclusion Filters** (filtres d'exclusion par défaut).

Étape 2 Pour créer un filtre d'exclusion, cliquez sur **Add Exclusion Filter** (Ajouter un filtre d'exclusion).

Étape 3 Préciser les paramètres des flux à exclure de la prise en compte lors de la découverte des politiques :

Vous n'avez pas besoin de saisir des valeurs pour tous les champs. Tout champ vide est traité comme un caractère générique pour les flux correspondants.

Toute conversation correspondant à tous les champs d'un filtre d'exclusion est ignorée lors de la création de la politique et de la mise en grappe.

Option	Description
Consumer	Correspond aux conversations pour lesquelles l'adresse du consommateur est membre de la portée sélectionnée, du filtre d'inventaire ou de la grappe (pour les filtres d'exclusion spécifiques à l'espace de travail uniquement). Vous pouvez spécifier n'importe quel espace d'adresse en créant un nouveau filtre personnalisé.
Provider	Correspond aux conversations pour lesquelles l'adresse du fournisseur est membre de la portée sélectionnée, du filtre d'inventaire ou de la grappe (pour les filtres d'exclusion spécifiques à l'espace de travail uniquement). Vous pouvez spécifier n'importe quel espace d'adresse en créant un nouveau filtre personnalisé.
Protocol	Correspond aux conversations avec le protocole spécifié.
Port	Correspond aux conversations avec le port du fournisseur (serveur) correspondant au port ou à la plage de ports spécifié. Saisissez les plages de ports en utilisant un tiret, par exemple « 100-200 »

Étape 4 Pour modifier ou supprimer un filtre d'exclusion, survolez la ligne applicable pour voir les boutons **Modifier** et **Supprimer**.

Étape 5 Si vous configurez des filtres d'exclusion par défaut :

Lorsque les filtres configurés sont prêts à l'emploi, revenez à la page **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut) et cliquez sur **Save** (enregistrer) pour rendre les modifications disponibles pour les espaces de travail individuels.

Prochaine étape

Important Les filtres d'exclusion sont activés par défaut dans l'espace de travail dans lequel ils sont configurés.

Les filtres d'exclusion par défaut sont activés par défaut dans tous les espaces de travail.

Les deux types de filtres d'exclusion sont activés par défaut dans la configuration de découverte des politiques par défaut.

Avant de découvrir les politiques :

- Activer ou désactiver les filtres d'exclusion et les filtres d'exclusion par défaut.
  - Dans chaque espace de travail
  - Dans la page de configuration de la découverte des politiques par défaut :

  Pour plus d'informations sur les instructions, consultez Activer ou désactiver les filtres d'exclusion, à la page 462
- Validez toute modification de portée, sinon les filtres pourraient ne pas correspondre (et donc exclure) les flux attendus. Consultez Valider les modifications, à la page 377.

Activer ou désactiver les filtres d'exclusion

Vous pouvez créer des filtres d'exclusion dans chaque espace de travail et/ou créer un ensemble de filtres d'exclusion par défaut que vous pouvez appliquer à tous les espaces de travail.

Par défaut, les deux types de filtres d'exclusion sont activés.

Pour apporter des modifications

- Pour activer ou désactiver les filtres d'exclusion pour un seul espace de travail :

  Dans l'espace de travail, cliquez sur **Manage Policies (Gérer les politiques)**, sur **Automatically Discover Policies (Découvrir automatiquement les politiques)**, puis sur **Advanced Configurations (Configurations avancées).** Vous pouvez activer des filtres d'exclusion ou des filtres d'exclusion par défaut pour cet espace de travail.

- Pour activer ou désactiver les filtres d'exclusion dans la configuration de découverte des politiques par défaut :

  Choisissez **Defend > Segmentation (défendre la segmentation)**, puis cliquez sur le signe d'insertion dans la partie droite de la page pour développer le menu Tools (outils). Choisissez ensuite **Default Policy Discovery Config (Configuration de la découverte des politiques par défaut).** Faites défiler la liste jusqu'à **Configurations avancées**, ou cliquez dessus. Vous pouvez activer des filtres d'exclusion et/ou des filtres d'exclusion par défaut.

Dépendances externes

Les dépendances externes ne sont pertinentes que lorsque vous utilisez le processus décrit dans (Avancé) Créer des politiques de portées croisées, on page 523.

Les paramètres de dépendances externes s'appliquent aux politiques découvertes automatiquement et impliquant des communications vers et depuis des charges de travail qui sont membres d'une portée autre que celle dans laquelle les politiques sont découvertes. (C'est-à-dire les communications impliquant des « charges de travail externes »).

Une charge de travail qui n'est pas membre de la portée dans laquelle la politique existe est une *charge de travail externe*. Ces charges de travail constituent l'autre extrémité d'une conversation avec une *charge de travail cible* (qui *est* membre de la portée dans laquelle la politique existe).

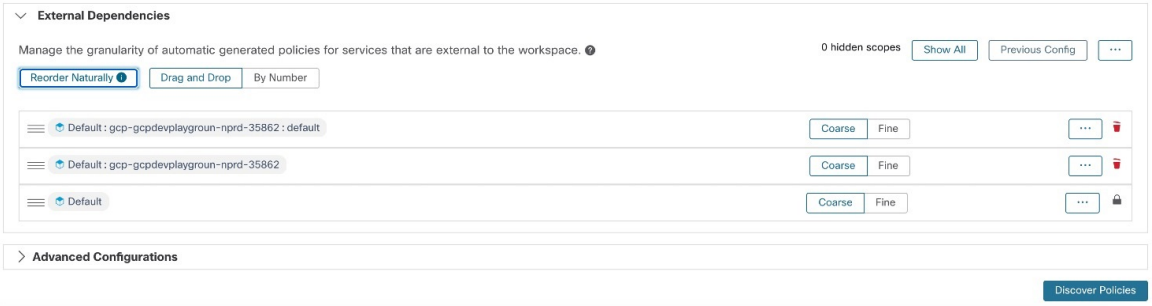
La liste des dépendances externes est une liste ordonnée de tous les portées de votre hiérarchie. Chaque portée de la liste est définie sur l'une des options suivantes :

- Générer des politiques spécifiques ou affinées (plus sécurisées), OU
- Générer des politiques plus globales dans des portées plus élevées, qui peuvent mieux se généraliser (c'est-à-dire qui sont plus susceptibles d'autoriser des flux légitimes qui n'ont pas été vus dans la plage temporelle spécifiée lors de la découverte des politiques).

Lors de la découverte de politique, la première portée (ou filtre de grappe ou d'inventaire - voir ci-dessous) qui correspond à la charge de travail sera utilisé pour générer la politique « autoriser », où l'ordre de correspondance (et le niveau de granularité qui en découle) est déterminé par le classement affiché dans la section Dépendances externes.

Un ordre des portées par défaut est configuré à votre intention, avec toutes les portées définies sur « globales » par défaut.

Figure 253: Dépendances externes par défaut



Destinataire	Faire ceci
Afficher ou affiner les dépendances externes pour un espace de travail :	Accédez à l'espace de travail et cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques), puis sur **External Dependencies** (Dépendances externes). Pour réorganiser les portées et choisir des options granulaires pour chacune, consultez Ajuster les dépendances externes d'un espace de travail, on page 464.
Configurez les dépendances externes par défaut pour la portée racine complète :	Consultez Configuration de la découverte de politiques par défaut, on page 477.

Dépendances externes : politiques granulaires impliquant des sous-ensembles de portées

Vous pouvez éventuellement découvrir des politiques à un niveau plus granulaire que le niveau de portée à portée, afin de contrôler le trafic vers un sous-ensemble spécifié de charges de travail dans une portée.

Par exemple, vous pouvez créer des politiques spécifiques à un certain type d'hôte au sein d'une application, comme les serveurs API ; vous pouvez regrouper ces charges de travail dans un sous-ensemble au sein de la portée de l'application.

Pour générer des politiques spécifiques à un sous-ensemble de charges de travail dans une portée, consultez Ajuster les dépendances externes d'un espace de travail, on page 464.

Conseils pour l'exploration des dépendances externes

Utilisez les conseils suivants pour explorer le comportement de la découverte automatique des politiques pour les politiques impliquant des espaces de travail qui ne sont pas membres de la portée associée à l'espace de travail dans lequel les politiques se trouvent.

Astuces

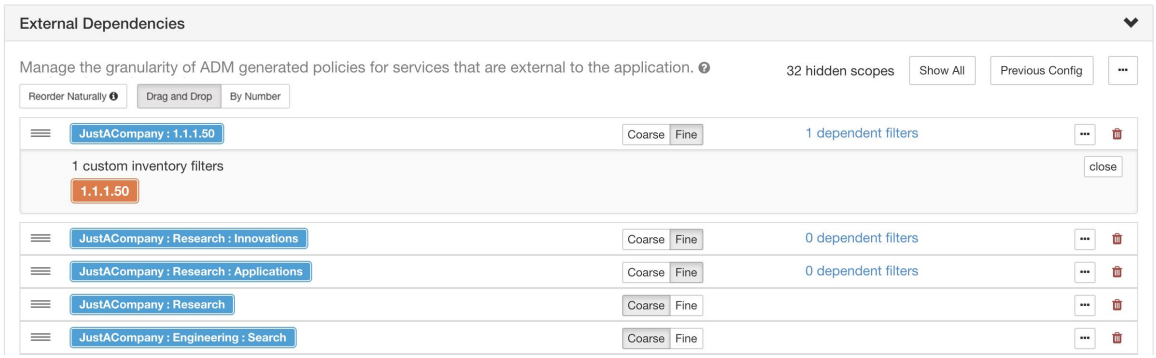
- Vous pouvez supprimer et réorganiser la liste pour générer des politiques avec la granularité souhaitée. Par exemple, la suppression de tous les sous-portées d'entreprise : RTP permettra de générer des politiques portées pour l'ensemble de la portée Entreprise : RTP, mais pas ses composants individuels, tout en maintenant une granularité plus élevée pour la portée SJC de l'entreprise. En outre, vous pouvez cliquer sur le bouton **Fine** (Fin) à côté de n'importe quelle portée et voir s'il existe des candidats à une granularité plus fine définis dans cette portée.
- Par défaut, la portée racine est configurée comme l'entrée la plus basse dans la liste des dépendances externes, de sorte que la découverte automatique des politiques génère toujours des politiques pour des portées plus spécifiques, chaque fois que cela est possible. Au départ, pour afficher relativement peu de politiques générales, vous pouvez placer temporairement la portée racine au-dessus des dépendances externes. De cette façon, après la découverte automatique des politiques, vous verrez toutes les politiques externes de l'espace de travail se connecter à une seule portée, la portée racine (car chaque charge de travail externe est mappée à la portée racine). Le nombre de politiques générées qui en résulte est réduit et plus facile à examiner et à comprendre.
- Vous pouvez également regrouper temporairement toutes les charges de travail qui sont membres de la portée associée à l'espace de travail (« charges de travail internes ») en une seule grappe, approuver la grappe, puis découvrir les politiques. Là encore, l'ensemble des politiques est réduit, car il n'y a pas de regroupement (subdivision de l'espace de travail/de la portée). Vous pouvez donc voir les politiques internes (connexion à des charges de travail internes) ou externes (connexion d'une charge de travail interne à une charge de travail externe). Ultérieurement, vous pourrez afficher des politiques de plus en plus affinées en dissociant les charges de travail internes et en disposant une ou plusieurs portées d'intérêt externes au-dessus de la racine.
- **important** Examinez toujours attentivement les politiques impliquant la portée racine, car ces politiques autorisent tout le trafic vers et à partir de l'ensemble du réseau. Cela est particulièrement important lorsque la portée racine est placée en bas de la liste des dépendances externes et que vous n'avez pas l'intention de générer des politiques générales. De telles politiques peuvent ne pas avoir résulté du trafic à l'échelle du réseau entrant ou sortant de la portée de l'espace de travail. Elles peuvent plutôt être déclenchées par quelques points terminaux externes qui n'ont pas réussi à recevoir des portées plus précises ou des affectations de filtres d'inventaire au-delà de la simple portée racine.

  Lors de l'audit de ces politiques, vous devez examiner les conversations associées (voir la section Conversations) pour identifier ces points terminaux, puis les classer en portées plus fines ou en filtres d'inventaire, pour éviter des politiques moins sécurisées au niveau de la portée racine.

Ajuster les dépendances externes d'un espace de travail

Cette procédure permet de créer des politiques entre des sous-ensembles spécifiés de charges de travail au sein de portées (plutôt qu'entre des portées entières) lors de la découverte automatique de politiques, lorsque le fournisseur d'une politique appartient à une portée différente de celle dans laquelle les politiques sont découvertes.

Illustration 254 : Réglage fin des dépendances externes



Avant de commencer

- Configurez un filtre d'inventaire pour chaque sous-ensemble de charges de travail pour lequel vous souhaitez générer des politiques spécifiques. Vous pouvez créer n'importe quel nombre de filtres d'inventaire, dans n'importe quelle portée.

  Il existe plusieurs façons de créer des filtres d'inventaire :

  - Convertir les grappes d'intérêt en filtres d'inventaire.

    (voir Convertir une grappe en filtre d'inventaire, à la page 510),

    et/ou

  - Créez de nouveaux filtres d'inventaire.

    Consultez Créer un filtre d'inventaire, à la page 392.

  Ces filtres doivent avoir les options suivantes activées :

  - **Restrict query to ownership scope**(Limiter la requête à la portée de la propriété)

    Provides a service external of its scope(Fournit un service hors de sa portée)

- Consultez aussi Conseils pour l'exploration des dépendances externes, à la page 463.

Procédure

Étape 1 Accédez à l'espace de travail dans lequel vous découvrirez les politiques.

Étape 2 Cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques).

Étape 3 Cliquez sur **External Dependencies** (Dépendances externes).

Étape 4 Si nécessaire, cliquez sur **Show All scopes** (Afficher toutes les portées).

Étape 5 (Facultatif) Exploiter les configurations précédentes :

- Pour réutiliser les modifications que vous avez apportées à la liste la dernière fois que vous avez détecté les politiques, cliquez sur **Previous Config** (Configuration précédente).
- Si vous avez configuré des dépendances externes dans la configuration par défaut de découverte des politiques par défaut, vous pouvez utiliser la liste globale en cliquant sur **Default Config** (Configuration

par défaut). Ou, après avoir obtenu la liste par défaut, vous pouvez la modifier comme vous le souhaitez (pour cet espace de travail uniquement), puis utiliser la version personnalisée lors des exécutions suivantes en cliquant une fois sur **Previous Config** (Configuration précédente).

Étape 6 Réorganiser les portées (et les filtres d'inventaire, le cas échéant) selon les besoins.

La politique est appliquée sur la base de la première portée ou du premier filtre d'inventaire de la liste (en commençant par le haut) qui correspond au trafic. À cette fin, vous souhaitez généralement appliquer la politique la plus spécifique qui corresponde au trafic, et vous voulez donc que les portées enfant (plus spécifiques) soient placées au-dessus de leurs parents (moins spécifiques).

- Si vous avez récemment créé de nouvelles portées enfants, qui sont par défaut ajoutées au bas de la liste, réorganisez la liste entière pour placer les portées enfants au-dessus de leurs parents :

  (Recommandé) Cliquez sur **Reorder Naturally** (Réorganiser naturellement).

  Illustration 255 : Réorganiser naturellement

- (Si vous avez une raison précise) Pour réorganiser la liste manuellement :
  - Cliquez sur **Drag and Drop** (Glisser et déposer).
  - Cliquez **By Number** (Par numéro) :

    Les dépendances externes se verront attribuer des valeurs de priorité par multiples de 10. Modifiez les valeurs pour modifier l'ordre.

    Une fois les numéros modifiés, cliquez sur **View** (afficher) pour mettre à jour l'ordre de la liste et réaffecter des multiples de 10 à chacune des priorités.

Étape 7 Précisez la granularité pour chaque ligne :

- Cliquez sur **Fine** (fine) pour chaque ligne pour laquelle vous souhaitez générer des politiques spécifiques aux filtres d'inventaire ou aux grappes configurés.

  Cliquez sur **Coarse** (grossière) pour générer des politiques qui s'appliquent à l'ensemble de la portée.

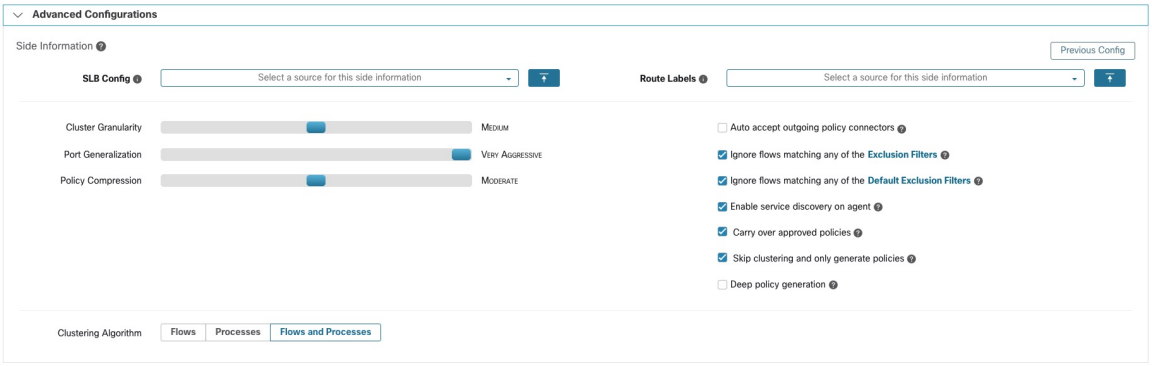
- Pour appliquer la granularité à toutes les sous-portées d'une portée : Cliquez sur le ··· situé à la fin de la ligne de la portée.

Configurations avancées pour la découverte automatique des politiques

Utilisez les paramètres avancés pour inclure des informations supplémentaires lors de la découverte de politiques ou pour vous adapter à un environnement particulier.

- Pour accéder à ces paramètres pour un espace de travail spécifique, cliquez sur **Automatically Discover Policies** (Découvrir automatiquement les politiques) dans l'espace de travail applicable.
- Pour modifier les valeurs par défaut de tous les espaces de travail, consultez Configuration de la découverte de politiques par défaut, on page 477.

Figure 256: Configurations avancées de découverte automatique des politiques



Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques

Vous pouvez charger des données à partir d'équilibreurs de charge et de routeurs pour fournir des éléments à la découverte automatique des politiques.

Pour accéder aux options suivantes, cliquez sur **Advanced Configurations** (Configurations avancées) dans les paramètres de découverte automatique des politiques et consultez la section « Side Information » ou « sideinfo » (Renseignements complémentaires).

Option	Description
Configuration SLB (Télécharger les configurations de l'équilibreur de charge)	Pour télécharger des données de votre équilibreur de charge dans le format correct, consultez Récupération des configurations de LoadBalancer pour la configuration de découverte avancée de politiques. Formats pris en charge pour le chargement des configurations de l'équilibreur de charge : • **F5 BIG-IP** • **Citrix Netscaler** • **HAProxy** • Autres : Utilisez le schéma **JSON normalisé**. Vous devez convertir toute configuration d'équilibreur de charge non prise en charge dans ce schéma. Ce schéma simple comprend des informations de base sur les adresses IP virtuelles (VIP) et les adresses IP principales. Pour télécharger un exemple de fichier JSON, cliquez sur le bouton d'informations à côté de **SLB Config** (Configuration SLB).
Charger des **étiquettes de routage**	Vous pouvez téléverser une liste de sous-réseaux/routes mis à disposition à partir des routeurs pour aider à partitionner les hôtes en fonction d'un ensemble de sous-réseaux pré-mis à disposition. Les résultats de mise en grappe générés par la découverte automatique des politiques ne dépassent jamais les limites du sous-réseau telles que définies par les données téléversées. Vous pouvez modifier les résultats une fois la découverte automatique des politiques terminée. Pour télécharger un exemple de fichier JSON, cliquez sur le bouton Renseignements à côté de **Route Labels** (étiquettes de routage).

Note Les grappes ne franchissent pas les limites des partitions, ce qui signifie qu'une grappe calculée par la découverte automatique de politiques ne contient pas de charges de travail cibles provenant de deux partitions différentes. Les partitions sont calculées à partir des données de l'équilibreur de charge ou du routeur téléversées. Cependant, vous pouvez déplacer librement les charges de travail d'une grappe à une autre, par exemple en modifiant les définitions de requête de grappe (modification manuelle de la grappe), ou désactiver le chargement de toutes les informations complémentaires.

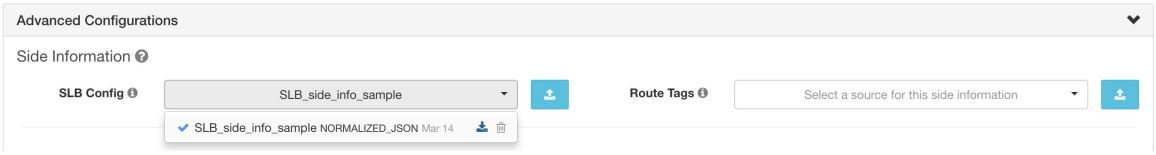
Pour afficher ou supprimer un fichier d'équilibreur de charge (configuration SLB) ou d'étiquettes de routage précédemment téléversé :

1. Cliquez dans la zone respective intitulée **Select a source for this side information** (Sélectionnez une source pour ces informations complémentaires).

   Une liste des fichiers téléversés apparaîtra.

2. Cliquez sur l'icône de téléchargement ou de corbeille à côté du fichier à afficher ou à supprimer.

Figure 257: Informations complémentaires téléversées



Granularité de la grappe

La granularité de la mise en grappe vous permet de contrôler la taille des grappes générées par la découverte automatique des politiques.

- **Fine** entraîne la formation d'un plus grand nombre de grappes, mais de taille plus réduite
- **Grossière** entraîne une diminution du nombre de grappes, mais une augmentation de leur taille

Note Vous pourriez ne pas observer de changement important dans les résultats en raison de nombreux autres signaux pris en compte par nos algorithmes. Par exemple, si le niveau de confiance des grappes générées est très élevé, la modification de ce contrôle modifiera peu les résultats.

Généralisation des ports

L'option de **Port Generalization** (généralisation de ports) dans **Advanced Configurations** (configurations avancées) pour la découverte automatique des politiques contrôle le niveau de signification statistique requis lors de la généralisation de ports, c'est-à-dire le remplacement de nombreux ports utilisés comme ports de serveur sur une seule charge de travail par un intervalle de port.

Ce paramètre peut avoir une incidence sur la précision, le nombre et la compacité des politiques ainsi que sur le temps nécessaire à leur génération.

Pour désactiver la généralisation de port, déplacez le curseur vers l'extrémité gauche. Notez que si elle est désactivée, la découverte automatique des politiques ou le temps de rendu de l'interface utilisateur de découverte automatique des politiques peut être considérablement réduit, si de nombreux ports de serveur sont utilisés par les charges de travail.

À mesure que le curseur se déplace vers la droite vers une généralisation plus audacieuse, moins de preuves sont nécessaires pour créer des intervalles de port et le critère de remplacement des politiques d'origine (impliquant des ports uniques) par des intervalles de port est assoupli.

Contexte

Certaines applications comme Hadoop utilisent et modifient de nombreux ports de serveur à un certain intervalle, par exemple entre 32000 et 61000. La découverte automatique des politiques tente de détecter ce comportement pour chaque charge de travail, en utilisant l'utilisation des ports de serveur de la charge de travail dans les flux observés : en observant seulement une fraction du total des ports possibles (mais de nombreux ports, par exemple des centaines), la découverte automatique des politiques peut « généraliser » que n'importe quel port entre, par exemple, 32000 et 61000, pourrait être utilisé comme port de serveur par la charge de travail. Les ports qui se trouvent à l'intérieur des intervalles sont remplacés par ces intervalles (lorsque certains critères relatifs aux nombres minimums observés sont remplis). Cela se traduit par moins de

politiques plus compactes. L'estimation de l'intervalle est importante pour le calcul de politiques précises : sans généralisation suffisante, de nombreux flux futurs légitimes seraient abandonnés si la politique est appliquée. En fusionnant de nombreux ports en un seul ou plusieurs intervalles, le temps de rendu de l'interface utilisateur est également considérablement réduit.

Vous pouvez contrôler le degré de généralisation des ports, y compris en le désactivant.

Compression des politiques

Lorsque la compression des politiques est activée, si les politiques de plusieurs grappes de l'espace de travail sont similaires, elles peuvent être remplacées par une ou plusieurs politiques applicables à l'ensemble de l'espace parent. Par exemple, si toutes ou presque les grappes de l'espace de travail fournissent le même port au même consommateur, toutes ces politiques spécifiques aux grappes sont remplacées par une seule politique dans la portée parente. Cela réduit considérablement le nombre de politiques, l'encombrement et peut également permettre des flux futurs légitimes qui auraient été abandonnés (généralisation précise).

Plus le paramètre de compression est élevé, plus le seuil requis pour la fréquence des politiques est bas afin de remplacer les politiques spécifiques aux grappes par une politique applicable à l'ensemble du parent.

lors de la génération de politiques pour une branche de l'arborescence de la portée :

Ce bouton peut être utilisé pour modifier le niveau de Compression hiérarchique des politiques.

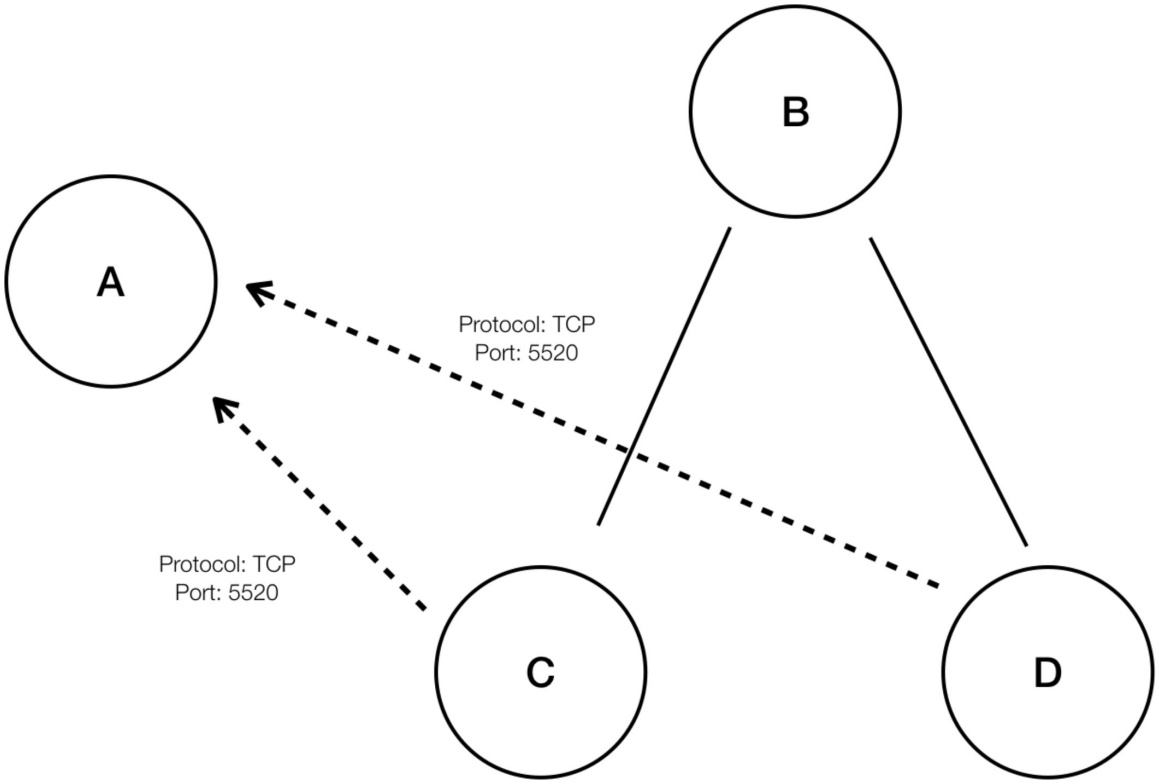
Note Actuellement, la page des conversations de découverte automatique des politiques ne permet pas d'afficher les conversations qui ont conduit à une politique compressée (vous devrez peut-être désactiver la compression ou utiliser la recherche de flux).

Compression hiérarchique des politiques

La compression des politiques peut également être effectué lors de la génération de politiques pour une branche de l'arborescence de la portée Le bouton Compression des politiques (Compression des politiques) peut être utilisé pour modifier le niveau de compression hiérarchique des politiques. Un exemple de compression hiérarchique des politiques est illustré ci-dessous.

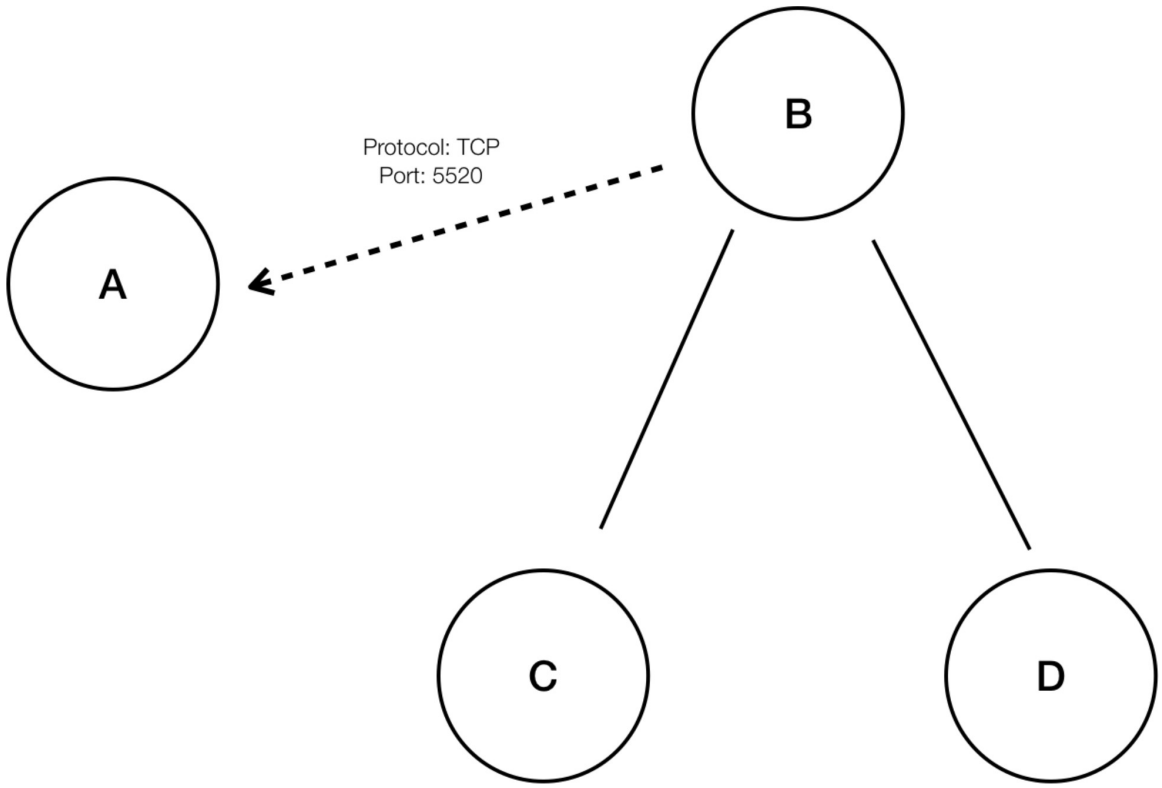
- Soit A, B, C et D, des portées faisant partie d'une arborescence de portées, où « C » et « D » sont les portées enfants de « B ». Soit « C » → » « A » soit une politique TCP « ALLOW (AUTORISER) » sur le port 5520 et « D » → » « A » soit la politique TCP « ALLOW » sur le port 5520.

Figure 258: Avant la compression hiérarchique des politiques



- Avec la compression hiérarchique des politiques, si un groupe suffisamment important de portées enfants implique des politiques partageant le même port, le même protocole et la même destination ou source, ces politiques seront remplacées par une politique généralisée qui relie la portée parente à la source ou à la destination commune. Dans le cas mentionné ci-dessus, « C » et « D » sont les portées enfants de « B » et les politiques « C » → » « A » et « D » → » « A » partagent la même destination, le même port et le même protocole. Étant donné que 100 % des portées enfants de « B » contiennent la politique similaire, la politique sera promue comme suit : « B » → » « A ». En outre, la compression hiérarchique peut être répétée afin qu'une politique généralisée puisse aller jusqu'à la racine de la sous-arborescence (branche de l'arborescence de la portée) .

Figure 259: Après la compression hiérarchique de la politique



- Le bouton Policy Compression (Compression de la politique) vous permet d'ajuster le degré de cette compression, en modifiant la proportion minimale requise des portées enfants partageant la politique (généralement mesurée en tant que fraction du nombre total de portées enfants) pour déclencher la compression. Lorsque cette option est désactivée, chaque politique est générée entre les portées de priorité la plus élevée en fonction de la liste des dépendances externes. Par la suite, si vous choisissez la liste des dépendances externes ordonnée naturellement, les politiques générées seront les politiques les plus granulaires parmi les portées.

Algorithme de mise en grappe (entrée de la mise en grappe)

Les utilisateurs avancés peuvent choisir la principale source de données pour les algorithmes de mise en grappe, c'est-à-dire les flux réseau en direct, ou l'exécution de processus, ou les deux.

Accepter automatiquement les connecteurs de politique sortants

Cette option s'applique uniquement lorsque vous utilisez la découverte automatique des politiques pour créer des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 523.

Toutes les demandes de politique sortantes créées lors de la découverte automatique des politique sont automatiquement acceptées.

Pour obtenir des renseignements complets, consultez Connecteurs de politiques d'acceptation automatique, on page 532 et la section Demandes de politiques.

Note Cette option est uniquement disponible pour les propriétaires de portée racine et les administrateurs de site.

Approuver automatiquement les politiques générées

Cette option est applicable si vous souhaitez approuver toutes les politiques générées par la découverte de politiques.

Note Sachez que si vous choisissez cette option, et plus tard si vous devez modifier ou annuler des modifications, vous ne pourrez le faire que manuellement.

Pour en savoir plus, consultez les Connecteurs de politiques d'acceptation automatique, on page 532 et Demandes de politiques.

Note Cette option est disponible pour les propriétaires d'portée racine et les administrateurs de site.

Ignorer les flux correspondants à des filtres d'exclusion

Pour ignorer les flux de conversation que vous spécifiez, activez l'option applicable. Pour afficher ou modifier l'une ou l'autre des listes de filtres, cliquez sur le lien **Exclusion Filters** (Filtres d'exclusion) applicables. Pour en savoir plus, consultez Filtres d'exclusion, Filtres d'exclusion par défaut, on page 478 et Configurer, modifier ou supprimer les filtres d'exclusion, on page 460.

Activer la découverte de service sur l'agent

Dans certaines applications, une large gamme de ports peut être désignée pour être utilisée, mais le trafic réel peut n'utiliser qu'un sous-ensemble de ces ports pendant la période de temps incluse dans la découverte de la politique. Cette option permet d'inclure l'ensemble du regroupement de ports désignés pour ces applications dans des politiques applicables à ces applications, plutôt que seulement les ports observés dans le trafic réel.

L'activation de cette option permet de recueillir des renseignements relatifs aux plages de ports éphémères concernant les services présents sur le nœud de l'agent. Des politiques sont ensuite générées en fonction de ces informations de plage de ports.

Exemple :

- Le serveur de domaine Windows Active Directory utilise la plage de ports éphémères Windows par défaut **49152 à 65535** pour traiter les demandes. Lorsque cet indicateur est défini, l'agent envoie des renseignements sur la plage de ports, et des politiques sont générées en fonction de ces informations.

Figure 260: Découverte de service activée sur l'agent

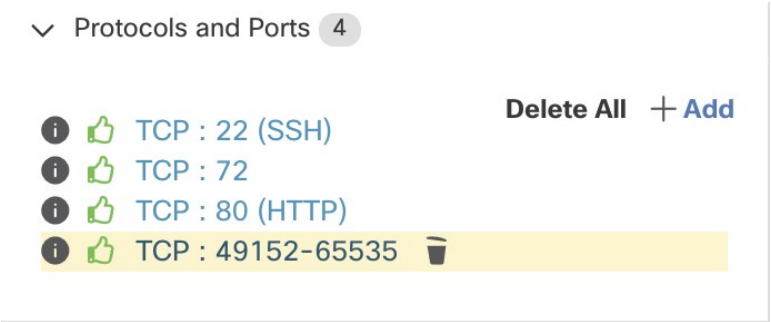
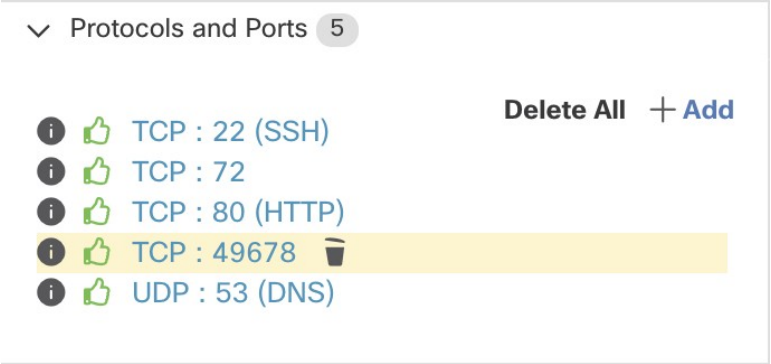


Figure 261: Découverte de service non activée sur l'agent



Reporter des politiques approuvées

Par défaut, cette option est activée.

Lorsque cet indicateur est défini, toutes les politiques que vous avez marquées comme approuvées (y compris celles approuvées à l'aide d'OpenAPI) seront conservées. Cela vous évite d'avoir à redéfinir une règle DENY de refus large particulière qui devrait prendre effet quelles que soient les politiques d'autorisation ALLOW détectées par la découverte automatique de politiques.

Pour de plus amples renseignements, consultez la section Politiques approuvées, on page 479.

Ignorer la mise en grappe et générer uniquement les politiques

Si cette option est sélectionnée, aucune nouvelle grappe n'est générée et les politiques sont générées à partir de toutes les grappes ou filtres d'inventaire approuvés existants et concernent l'ensemble de la portée associée à l'espace de travail (ce qui revient à traiter l'ensemble de la portée comme une seule grappe). Cette option permet de réduire considérablement le nombre de politiques (mais de les rendre plus approximatives).

Activer la suppression des politiques redondantes

Cette option n'est disponible que lors de la génération de politiques pour une branche de l'arborescence de la portée.

Cette option active/désactive la suppression des politiques granulaires redondantes.

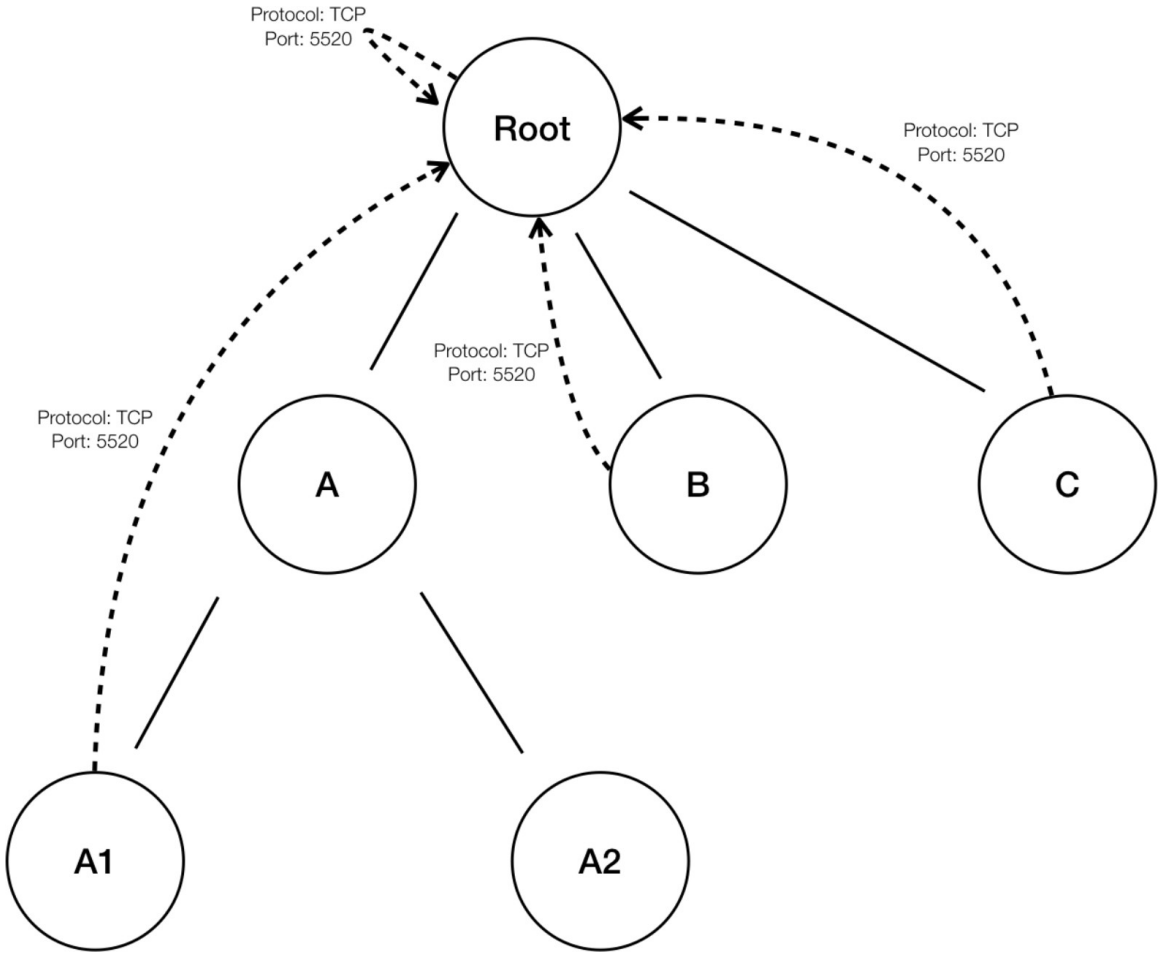
Exemple :

- Soit la racine Root, A, B, C, A1 et A2 des portées faisant partie d'une arborescence de portées. Soit les politiques suivantes :

  1. « Root » → « Root »
  2. « B » → « Root »
  3. « C » → « Root »

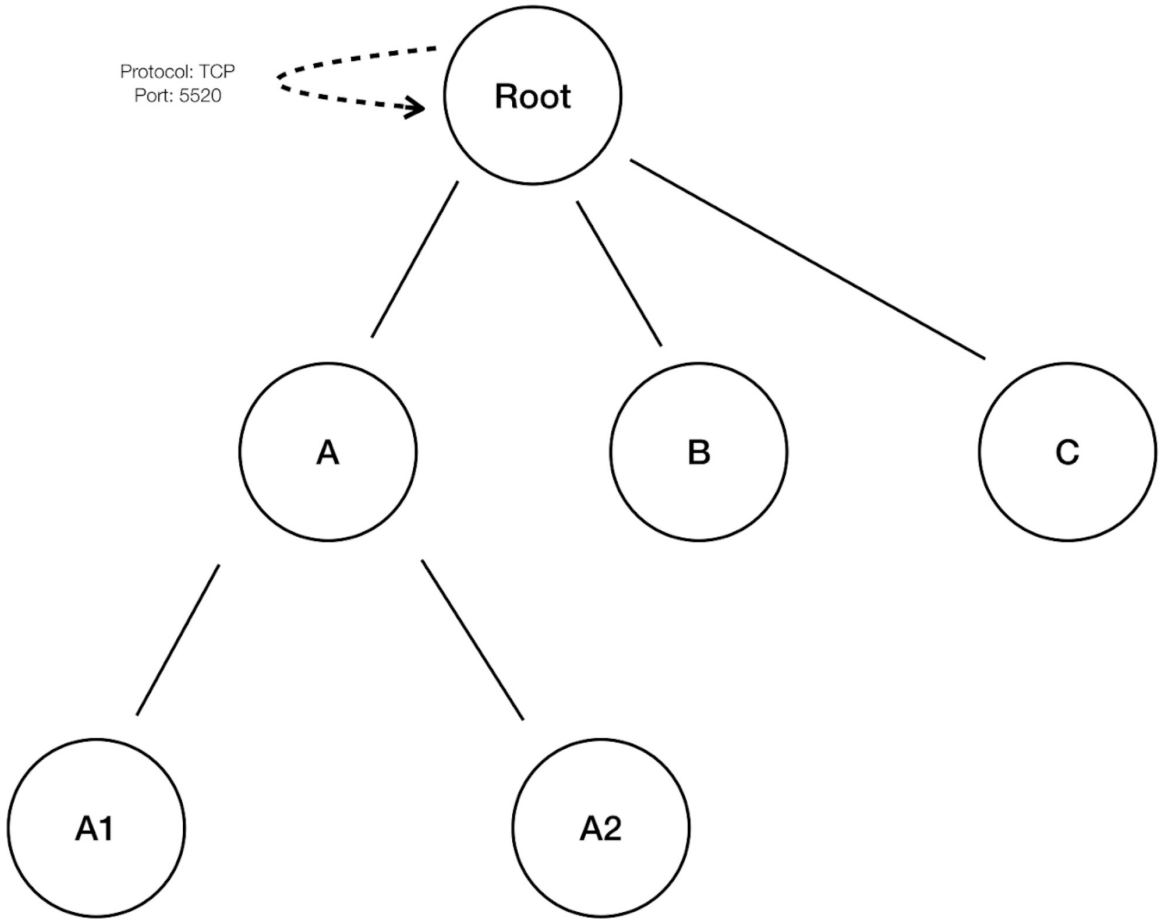
  4. « A1 » → « Root »

Figure 262: Avant la suppression des politiques redondantes



- Les politiques « B » →« Root », « C » →« Root » and « A1 »→ « Root » sont redondantes, car la politique « Root »→« Root » couvre ces politiques. La fonction de suppression des politiques redondantes vérifie et supprime ces politiques. Il n'y a donc qu'une seule politique, « Root »→ « Root », comme suit.

Figure 263: Après la suppression des politiques redondantes



La suppression des politiques redondantes peut être très utile pour conserver un ensemble succinct de politiques interprétables. L'ensemble de politiques réduit contient le nombre minimal de politiques au niveau de compression choisi pour couvrir tout le trafic de charge de travail. Cependant, vous devez toujours effectuer un audit de la politique au moyen d'une analyse des politiques et examiner les conversations correspondantes pour évaluer le caractère strict des politiques qui en résultent. Cela est particulièrement important lorsqu'il existe un trafic à destination ou en provenance des points terminaux qui ne sont pas classés dans des portées plus précises ou des filtres d'inventaire. Ces points terminaux peuvent déclencher la génération de politiques plus globales que prévu, comme des politiques impliquant la portée racine. Si la suppression des politiques redondantes est activée en même temps, les politiques plus granulaires seront supprimées et ne vous seront pas présentées. Pour diagnostiquer la source des politiques (compressées) et pour afficher les politiques de niveau plus précis, désactivez la compression des politiques et la suppression des politiques redondantes. Notez également qu'actuellement, la page des conversations de découverte automatique des politiques peut ne pas afficher les conversations qui mènent à une politique compressée/généralisée. Pour contourner ce problème, vous pouvez désactiver la compression et la suppression des politiques redondantes, afin qu'il soit plus facile de trouver les conversations qui mènent aux politiques générées.

Tip Étant donné que la - en découvrant les politiques pour une branche de l'arborescence de l'espace de travail - découvre toutes les politiques pour le sous-arborescence de l'espace de travail ayant pour racine l'espace de travail, ces politiques couvriront tout le trafic légal vu par la découverte automatique de politiques pour toutes les charges de travail sous la sous-arborescence. Lorsque vous analysez ces politiques à l'aide d'outils comme l'analyse des politiques (voir l'article sur les Politiques), vous devez désactiver l'analyse des politiques dans tous les espaces de travail associés aux sous-portées. De cette façon, les politiques (le cas échéant) résidant dans les espaces de travail de sous-portée (qui reçoivent généralement une priorité élevée en raison d'une définition de portée plus spécifique) ne seront pas prioritaires et n'interféreront pas avec les résultats. Cependant, des exceptions s'appliquent lorsque les politiques des espaces de travail de sous-portée sont configurées pour couvrir différents ensembles de trafic qui impliquent généralement des filtres d'inventaire plus fins ou des grappes spécifiques aux sous-portées.

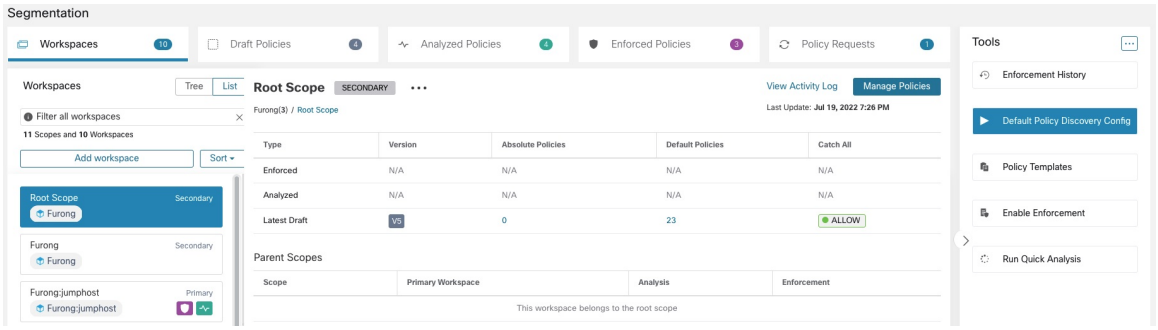
Configuration de la découverte de politiques par défaut

Vous pouvez configurer les paramètres de découverte automatique des politiques par défaut qui peuvent éventuellement être utilisés dans n'importe quel espace de travail dans l'ensemble de la portée racine.

Pour configurer les options par défaut pour la découverte de politiques :

Choisissez **Defend** > **Segmentation**(défendre la segmentation), puis cliquez sur le signe d'insertion dans la partie droite de la page pour développer le menu Tools (outils). Choisissez ensuite **Default Policy Discovery Config** (Configuration de la découverte des politiques par défaut).

Figure 264: Accès à la page de configuration de la découverte des politiques par défaut



Pour en savoir plus sur les options de la page de configuration de la découverte des politiques par défaut, consultez :

- Dépendances externes, on page 462 et les rubriques secondaires
- Configurations avancées pour la découverte automatique des politiques, on page 467 et les rubriques secondaires
- Filtres d'exclusion par défaut, on page 478

Important Lorsque vos configurations par défaut sont terminées et prêtes à l'utilisation dans des espaces de travail individuels, cliquez sur **Save** (Enregistrer).

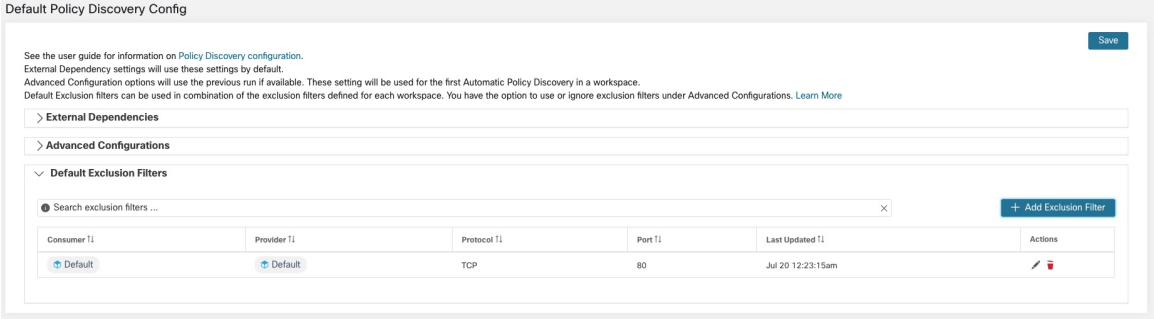
Filtres d'exclusion par défaut

Les filtres d'exclusion vous aident à affiner les politiques et les grappes suggérées par la découverte automatique des politiques en spécifiant les flux de trafic à exclure de l'entrée de la découverte.

Pour en savoir plus, consultez les Filtres d'exclusion.

Vous pouvez créer une liste globale des filtres d'exclusion par défaut qui soit disponible pour tous les espaces de travail de votre détenteur, puis préciser pour chaque espace de travail si vous souhaitez utiliser ou non cette liste par défaut lors de la découverte des politiques.

Figure 265: Filtres d'exclusion par défaut



Pour configurer les filtres d'exclusion par défaut, consultez Configurer, modifier ou supprimer les filtres d'exclusion, on page 460.

Pour activer ou désactiver les filtres d'exclusion par défaut, consultez Activer ou désactiver les filtres d'exclusion, on page 462.

Récupération des configurations de LoadBalancer pour la configuration de découverte avancée de politiques

Vous trouverez ci-dessous des instructions pour récupérer les fichiers de configuration d'équilibreur de charge pris en charge dans un format qui peut être directement téléversé dans Cisco Secure Workload pour une utilisation dans la découverte de politiques. Pour en savoir plus, consultez les sections Configurations avancées pour la découverte automatique des politiques et Inclure les données des équilibreurs de charge et des routeurs lors de la découverte des politiques, on page 467.

Notez que tous les fichiers doivent être encodés en ASCII.

Citrix Netscaler

Concaténez la sortie de `show run` dans votre console et téléchargez le fichier.

Voir un exemple de fichier de configuration

F5 BIG-IP

Chargez le fichier `bigip.conf`.

Note Si vous possédez un fichier avec une extension .UCS, décompressez le dossier d'archive et chargez uniquement le `fichier bigip.conf` dans la vidage de configuration. S'il existe plusieurs `fichiers bigip.conf`, concaténez-les, puis téléchargez-les.

Voir un exemple de fichier de configuration

HAProxy

Chargez votre fichier `haproxy.cfg`. Le chemin d'accès est généralement `/etc/haproxy/haproxy.cfg`.

Voir un exemple de fichier de configuration

JSON normalisé

Si vous trouvez que les options ci-dessus sont contraignantes, convertissez vos configurations selon le schéma JSON suivant et téléversez-les directement. L'exemple de fichier JSON peut être téléchargé directement en cliquant sur l'icône **i** à côté de Configuration SLB Config dans Configurations d'exécution avancées pour la découverte automatique des politiques.

Voir un exemple de fichier de configuration

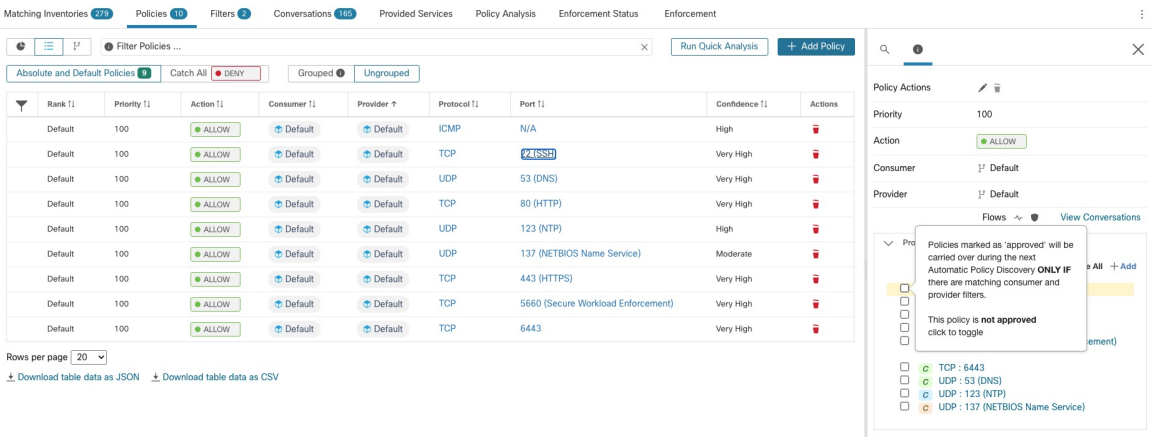
Approuver les politiques

Lorsque vous passez en revue les résultats de la découverte des politiques, approuvez les politiques découvertes que vous souhaitez conserver pour les conserver telles quelles lorsque vous découvrirez des politiques ultérieurement. Pour en savoir plus, consultez Politiques approuvées, à la page 479.

Pour approuver une politique :

1. Dans la page Policies (Politiques), pour la politique que vous souhaitez protéger, cliquez sur la valeur dans la colonne **Protocols and Ports** (Protocoles et Ports).
2. Dans le panneau qui s'ouvre sur la droite, cochez la case à gauche de chaque protocole et port pour lesquels vous souhaitez conserver la politique lors de la découverte future de politiques.

Illustration 266 : Approuver les politiques



Vous pouvez également utiliser cette procédure pour supprimer l'approbation d'une politique.

Politiques approuvées

En général, les politiques approuvées ne sont pas modifiées lors de la recherche automatique de politiques, et cette dernière ne suggère pas de politiques qui feraient double emploi ou chevaucheraient les effets des politiques approuvées.

Les politiques suivantes sont approuvées :

- Les politiques créées manuellement.

- Les politiques découvertes qui sont approuvées manuellement

  (Lorsque vous êtes convaincu qu'une politique se comporte comme prévu, vous l'approuvez pour la protéger contre les modifications lors de la future découverte automatique des politiques. Voir Approuver les politiques, on page 479).

- Politiques téléversées, à moins qu'elles ne soient explicitement marquées comme `approuvées : faux`.

- Les politiques approuvées qui sont définies dans les portées parent et ancêtre (en particulier, à partir des dernières versions de leurs espaces de travail principal) qui s'appliquent aux charges de travail de cette portée.

- Les politiques créées lorsque des demandes de politique sont acceptées à partir d'un autre espace de travail, lorsque des politiques à portée croisée sont gérées à l'aide de la méthode avancée décrite dans Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, on page 522. Par exemple, cela inclut les politiques incluses à partir de l'onglet Services fournis, on page 534.

Les politiques approuvées sont accompagnées d'une icône représentant un pouces vers le haut à côté du type de protocole lorsque vous cliquez sur les liens des ports ou des protocoles d'une politique et que vous affichez les détails dans le panneau à droite de la page.

Exceptions aux protections de politiques approuvées

Les politiques approuvées sont conservées lors de la découverte automatique future des politiques si *les deux* extrémités de la politique sont parmi les suivantes : grappe approuvée; filtre d'inventaire; demande de politique acceptée (pour les politiques couvrant plusieurs portées); ou grappe qui ne modifie pas de manière significative les membres. (Cependant, les membres de la grappe peuvent avoir changé dans le dernier cas).

Les politiques approuvées pourraient ne pas être protégées lors des futures exécutions de découverte automatique des politiques si l'une des extrémités des politiques est une grappe qui n'est pas approuvée et si, lors de la découverte automatique des politiques, aucune nouvelle grappe générée ne présente un chevauchement suffisamment élevé avec cette grappe.

Pour protéger une politique qui implique une grappe non approuvée, vous devez approuver explicitement les grappes à chaque extrémité de la politique.

Il existe également une configuration avancée pour la découverte automatique des politiques qui est activée par défaut. Si vous ne souhaitez pas protéger les politiques approuvées contre les modifications, vous pouvez désélectionner cette option pour un espace de travail ou pour la configuration de découverte de politiques par défaut globale :. Consultez Reporter des politiques approuvées, on page 474.

Dépanner les politiques approuvées

Les politiques approuvées ne sont pas reportées

Si les politiques approuvées ne sont pas reportées comme prévu, assurez-vous que l'option de report **des politiques approuvées** est sélectionnée dans les paramètres de configuration avancés ou par défaut pour la découverte automatique des politiques.

Trouver les conversations exclues de la génération de politiques

Lors de la découverte automatique des politiques, toutes les conversations correspondant aux critères d'une politique approuvée existante sont exclues de la génération de politique. Cette omission empêche la génération de politiques redondantes couvrant les mêmes conversations. (Ce processus diffère des filtres d'exclusion

(voir la section Filtres d'exclusion), dans laquelle vous définissez des filtres de correspondance au lieu de politiques. Les filtres d'exclusion empêchent les conversations correspondantes d'être visibles dans toutes les parties de la découverte automatique des politiques.)

Notez que même si des politiques redondantes ne sont pas générées à partir de ces conversations, celles-ci sont toujours prises en compte lorsque la découverte automatique des politiques analyse et génère des grappes.

Pour voir quelles conversations sont exclues de la découverte automatique des politiques par les politiques approuvées existantes :

Dans l'affichage des conversations (voir l'article Conversations), utilisez l'indicateur d'**exclusion** pour filtrer les conversations. Vous pouvez également voir quelles politiques approuvées existantes entraînent l'exclusion de ces conversations dans la vue détaillée de la politique qui s'ouvre sur le côté droit de la page lorsque vous cliquez sur le lien Ports et protocoles dans une politique, puis sur l'icône d'exclusion à côté de la conversation. (Survolez les icônes pour trouver l'icône appropriée).

Réviser les politiques de manière itérative

La définition et la précision des politiques, pour une portée unique et pour l'ensemble d'un réseau, constituent un processus itératif.

Vous pouvez vous attendre à réviser à la fois les politiques découvertes et celles créées manuellement.

Réexécution de la découverte automatique des politiques

Vous pouvez réexécuter la découverte automatique des politiques à tout moment. Les raisons principales de réexécuter la recherche automatique de politiques sont d'inclure des renseignements supplémentaires qui n'ont pas été inclus dans l'exécution précédente, ou d'exclure des renseignements qui ne sont pas utiles. Par exemple, vous pouvez :

- Installer des agents supplémentaires ou configurer des connecteurs supplémentaires et permettre à certaines données de flux de s'accumuler.
- Augmenter la durée utilisée pour la découverte, afin d'inclure davantage de données.
- Approuver les grappes (avec ou sans modification au préalable), ce qui peut améliorer la mise en grappe d'autres charges de travail lors de la réexécution. Consultez Approbation des grappes, on page 514.
- Exclure les flux dont vous savez que vous ne voulez pas influencer la politique afin de ne pas avoir à les supprimer. Consultez Filtres d'exclusion, on page 459.
- Modifier les paramètres avancés (pour en savoir plus, voir Configurations avancées pour la découverte automatique des politiques, on page 467).
- Capturer les modifications après avoir modifié Aborder les complexités de la politique, on page 515.

La redécouverte automatique des politiques sur un espace de travail existant peut générer des grappes et des politiques différentes dans cet espace.

Si un hôte ne fait plus partie de la portée de l'espace de travail, il n'apparaîtra dans aucune grappe lors d'une exécution de découverte automatique des politiques ultérieure; S'il se trouve dans une grappe approuvée, il n'y apparaîtra plus. Même avec le même ensemble de charges de travail de membres, mais avec une configuration différente dans le temps, la découverte automatique des politiques peut générer différentes grappes.

Note Pour obtenir la liste des types de politique qui ne sont pas modifiés lors de la découverte de la politique, consultez Politiques approuvées, on page 479.

Note *Suppression des politiques redondantes* Lors de la découverte automatique ultérieure de politiques, les politiques approuvées dans les espaces de travail principaux supprimeront les conversations correspondantes pour la génération de politiques, de sorte que des politiques redondantes ne seront pas générées. Notez que, comme c'est le cas pour les filtres d'exclusion, cette fonctionnalité peut ne pas fonctionner parfaitement sur les espaces de travail non principaux si la politique utilise un filtre de grappe défini dans l'espace de travail. Les filtres de grappe des espaces de travail non principaux ne sont pas actifs et ne correspondront à aucun flux. Par conséquent, des politiques redondantes peuvent toujours être générées dans ces espaces de travail lors de la découverte automatique des politiques.

Important : Avant de réexécuter la découverte automatique des politiques

Important Répondez aux questions suivantes avant de relancer la découverte des politiques dans un espace de travail :

- Par défaut, chaque fois que vous découvrez des politiques dans un espace de travail particulier, l'ensemble précédent de politiques et de grappes découvertes est remplacé en fonction des données incluses dans la nouvelle période de découverte. Si vous souhaitez conserver certaines politiques et certaines grappes, mais pas d'autres, approuvez ces politiques et ces grappes.
- Si vous souhaitez conserver les grappes générées existantes, consultez Prévention de la modification des grappes lors des réexécutions de découverte automatique des politiques ou Approbation des grappes, on page 514.
- Si vous souhaitez conserver les politiques générées existantes, consultez Approuver les politiques, on page 479.
- Tous les paramètres de configuration **avancée** existants configurés lors de l'exécution de découverte précédente sont utilisés, sauf si vous les modifiez.

  Cependant, toutes les dépendances externes configurées *par défaut* seront utilisées à la place de celles de l'exécution précédente.
- Si la version actuellement affichée des politiques découvertes n'est pas la dernière version et que vous souhaitez conserver les versions précédemment découvertes, cliquez sur la version affichée en haut de la page et choisissez la dernière version v*.

  Si une version précédente est affichée, toutes les versions comprises entre cette version et la nouvelle version découverte seront supprimées.

  Pour de plus amples renseignements, consultez la section Afficher, comparer et gérer les versions de politiques découvertes, on page 483.

Pour réexécuter la découverte de politique, consultez Découvrir automatiquement les politiques, on page 456. Une fois que vous avez abordé les points de cette rubrique, le processus est le même chaque fois que vous découvrez des politiques.

Afficher, comparer et gérer les versions de politiques découvertes

Chaque fois que vous découvrez des politiques dans un espace de travail, le numéro de version (v*) affecté à l'ensemble de politiques est incrémenté.

Pour en savoir plus, consultez À propos des versions des politiques (v* et p*), à la page 575.

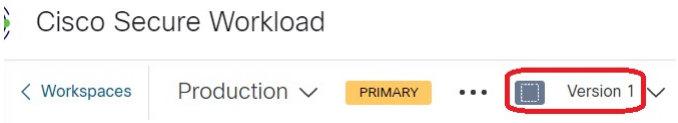
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez à l'espace de travail

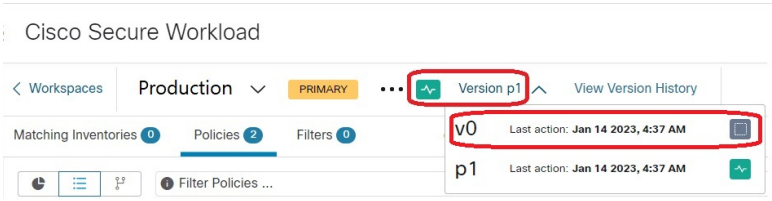
Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

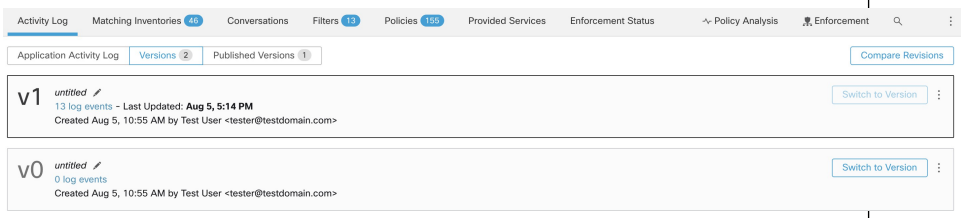
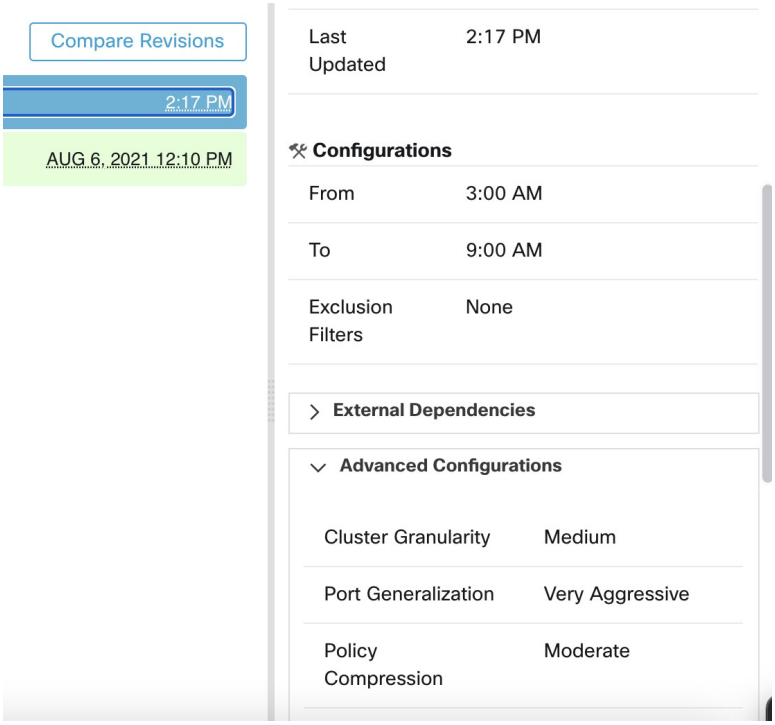
Étape 4 La version actuellement affichée des politiques générées par la découverte automatique des politiques est indiquée en haut de la page :



Si vous avez déjà analysé ou appliqué des politiques, la version affichée peut être une version de découverte de politiques, une version analysée ou une version appliquée.

Étape 5 Effectuez l'une des opérations suivantes :

Afficher une version différente des politiques générées par la découverte automatique des politiques :	Cliquez sur la version actuelle et choisissez une autre version v*. (Si des versions p* s'affichent, il s'agit de versions analysées et/ou appliquées, et non de versions des politiques découvertes).  **Important!** Consultez la mise en garde dans la section Que faire ensuite à la fin de cette procédure.

Afficher les détails d'une version	**1.** Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. **2.** Cliquez sur l'onglet **Versions** pour voir les versions des politiques détectées. (Il ne s'agit pas de l'onglet Published Versions (Versions publiées).) La liste des versions s'affiche : ***Illustration 267 : Liste des versions de politique générées avec des renseignements résumés***  **3.** Cliquez sur le lien **log events** (journal des événements) dans la version. **4.** Cliquez sur un lien dans une ligne d'événement. Les renseignements détaillés disponibles comprennent les statistiques, les filtres d'exclusion, les dépendances externes et les configurations pour l'exécution. ***Illustration 268 : Configurations utilisées pour des exécutions particulières de découverte automatique de politiques*** 

Comparez deux versions pour voir ce qui a changé :	**1.** Cliquez sur **Compare Revisions** (Comparer les révisions). **2.** Choisissez les versions à comparer. **3.** Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 577.
Supprimez une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Vous ne pouvez pas supprimer la dernière version générée par la découverte automatique des politiques (version v*).
Exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...)..

Prochaine étape

Important Si vous souhaitez conserver les versions précédentes des politiques découvertes, affichez toujours la version actuelle des politiques découvertes lorsque vous avez fini d'utiliser des versions plus anciennes.

Si la version la plus récente des politiques détectées ne s'affiche pas lors de la prochaine découverte des politiques pour cet espace de travail, les versions plus anciennes peuvent être supprimées.

Par exemple, si la version la plus récente des politiques découvertes est la v4 et que la version v2 s'affiche lorsque vous découvrez à nouveau des politiques, les versions v3 et v4 existantes seront supprimées, et la nouvelle version découverte sera la v3.

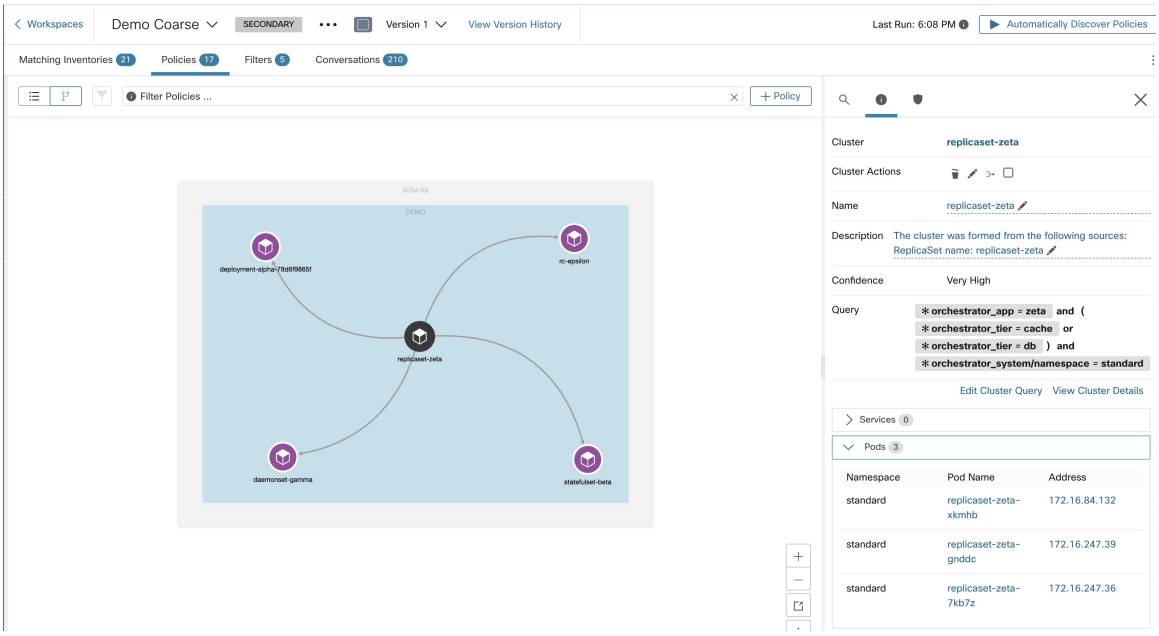
Ce comportement garantit un historique de version linéaire, ce qui simplifie le retour à une version précédente si vous le souhaitez.

En outre, vous ne pouvez créer manuellement des politiques que si la dernière version v* est affichée.

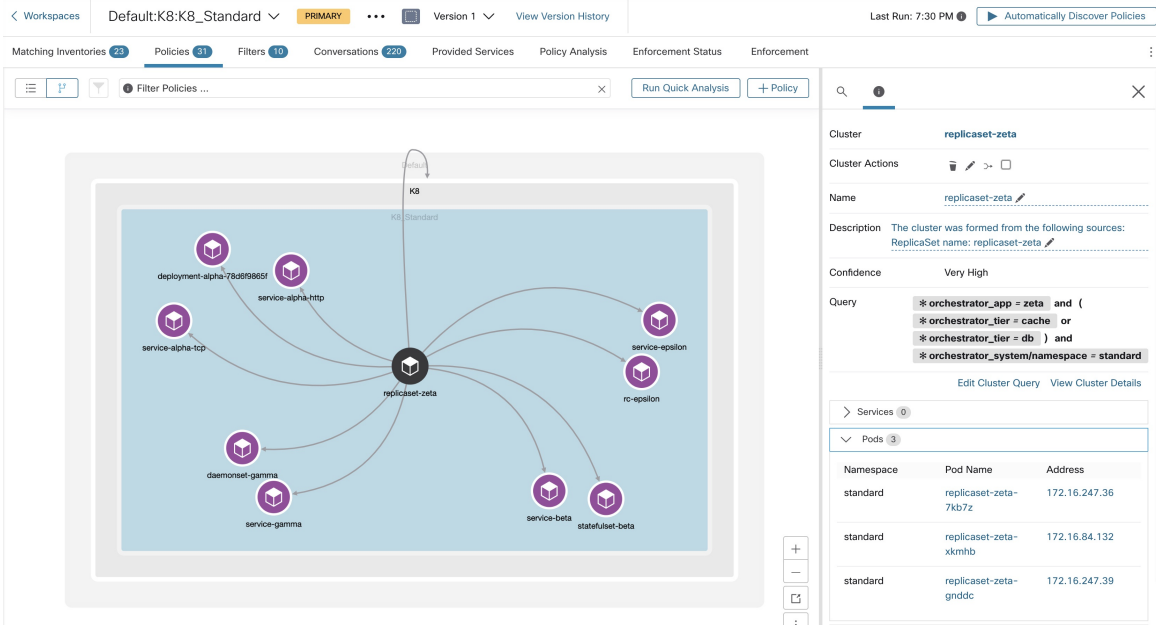
Soutien Kubernetes de la découverte des politiques

La découverte des politiques utilise les informations sur les pods et les services de la configuration Kubernetes pour créer des grappes à la fois pour les pods et les services et les politiques respectives sont générées.

Si la granularité de la grappe est COARSE (GROSSIÈRE) ou VERY COARSE (TRÈS GROSSIÈRE), les services et les pods qui les soutiennent sont mis en grappe ensemble.



Si la granularité de la grappe est définie sur moyenne, fine ou très fine, les services et les pods qui les soutiennent sont mis en grappe séparément.



Pour les grappes de pods, les informations sur la source sont ajoutées dans le cadre de la description de la grappe et chaque grappe de la description contient les informations sur l'entité à l'origine de la formation de la grappe.

Par exemple, **description** : « *La grappe a été formée à partir des sources suivantes : Nom de l'ensemble de réplications : ReplicaSet-zeta* ».

Importer/Exporter

Exporter un espace de travail

Tout le contenu pertinent des groupes et des politiques de chaque espace de travail peut être téléchargé en un fichier unique dans plusieurs formats de documents structurés couramment utilisés comme JSON, XML et YAML. Ces fichiers peuvent être utilisés pour un traitement ultérieur en interne ou pour être incorporés dans d'autres outils d'analyse ou d'application de la politique.

Accédez à l'élément du menu **...** dans l'en-tête de l'espace de travail et cliquez sur l'élément **export** (exporter). Cela affichera la boîte de dialogue d'exportation. Vous pouvez choisir si le fichier exporté doit inclure uniquement le contenu de la grappe ou de la grappe et des politiques de sécurité parmi les grappes générées par la découverte automatique des politiques en fonction des flux de réseau réels. Choisissez le format souhaité et cliquez sur download (télécharger) pour télécharger le fichier dans le système de fichiers local.

Figure 269: Éléments de menu Import/Export (Importer/Exporter)

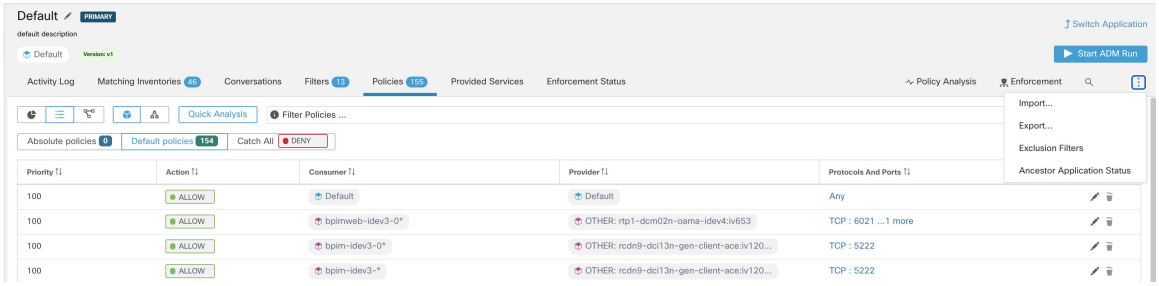
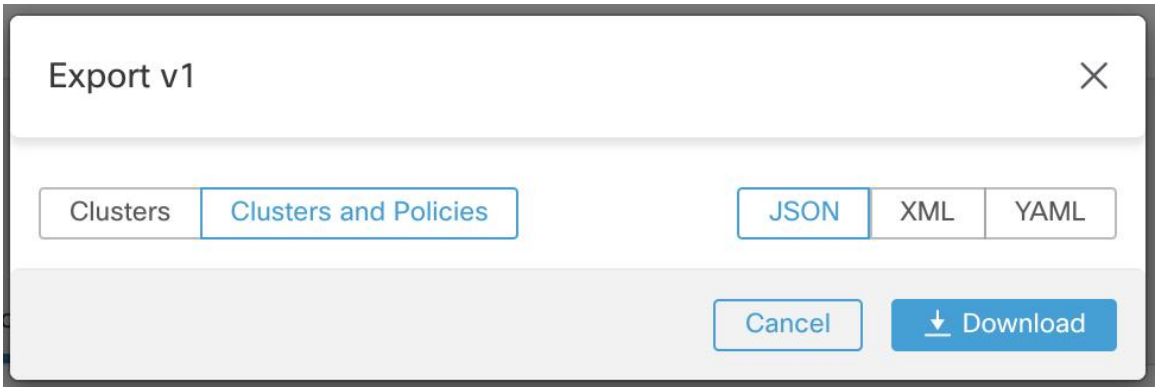


Figure 270: Exportation des politiques d'un espace de travail



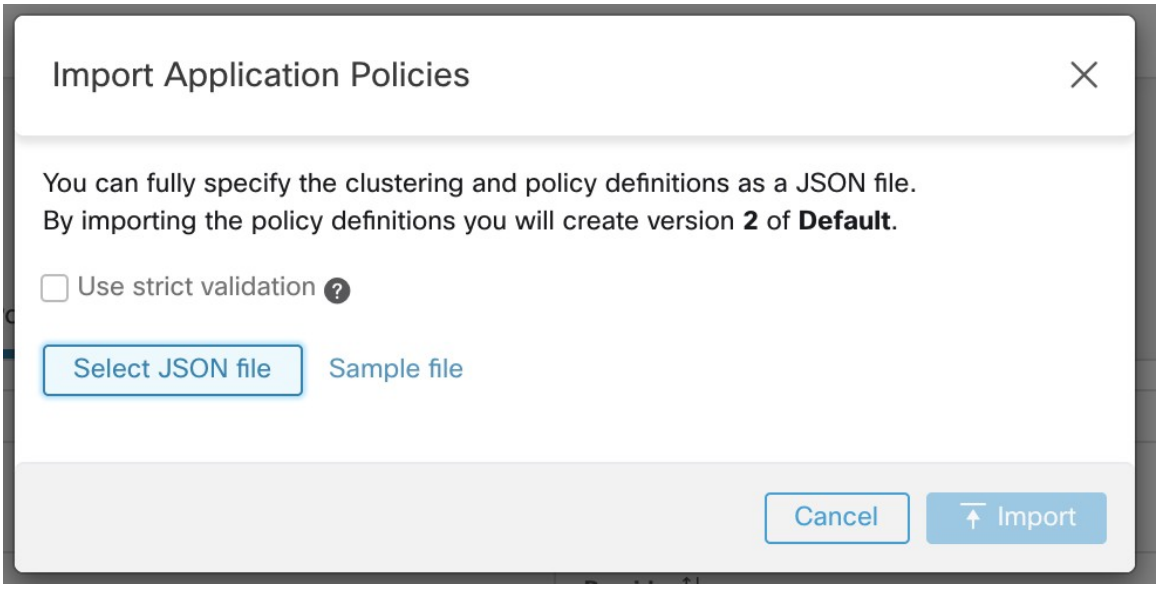
Lorsque vous exportez un espace de travail, le paramètre Auto accept outgoing policy connectors (« Accepter automatiquement les connecteurs de politique sortants ») dans la configuration de découverte automatique des politiques est inclus et sera actif dans l'espace de travail importé.

Importer

Vous pouvez importer des définitions connues de grappes et de politiques dans un espace de travail en chargeant directement un fichier JSON. Tout comme la découverte automatique des politiques, le chargement de politiques dans un espace de travail existant crée une nouvelle version et place la grappe et les définitions de politiques sous la nouvelle version. Les filtres manquants et les valeurs de propriété incorrectes renverront une erreur.

Cliquez sur l'élément de menu **Import** (Importer) dans **. . Menu** dans l'en-tête de l'espace de travail. Dans la boîte de dialogue d'importation, vous pouvez sélectionner un fichier JSON avec un format valide. Vous pouvez obtenir un petit exemple de fichier JSON illustrant le schéma pour les politiques et les grappes en cliquant sur le bouton **Example** (Exemple).

Figure 271: Importation des grappes et politiques



La validation stricte, si elle est activée, renverra une erreur si le JSON contient des attributs non reconnus. Ceci est utile pour localiser les fautes de frappe ou les champs facultatifs mal identifiés.

Note Toutes les politiques importées sont marquées comme approuvées par défaut, sauf si elles sont explicitement marquées comme `approved: false` (approuvées : faux). Vous avez la possibilité de maintenir ces politiques approuvées pendant la découverte automatique des politiques afin de générer un nouvel ensemble de politiques. Consultez Politiques approuvées, on page 479 pour en savoir plus.

Conseil de pro : Le schéma du fichier JSON récupéré lors de l'exportation d'un espace de travail d'application est compatible avec le schéma du format attendu pour l'importation de politiques dans un espace de travail. Par conséquent, vous pouvez copier les politiques d'un espace de travail d'application vers un autre en utilisant une exportation suivie d'une importation. Notez que de nombreuses fonctionnalités peuvent ne pas fonctionner de la même manière lors de l'exportation puis de l'importation de politiques. Par exemple, les conversations à l'appui des politiques ne sont pas incluses dans l'exportation et ne seront pas présentes lors de l'importation des politiques non plus.

Politiques spécifiques à la plateforme

Pour des renseignements importants sur la façon dont les agents appliquent les politiques sur chaque plateforme, consultez Application des politiques par le biais d'agents, à la page 55. Pour Kubernetes/OpenShift, consultez Application des conteneurs, à la page 566.

Windows

Configuration de politique basée sur le système d'exploitation Windows recommandée

toujours spécifier les ports et les protocoles dans les politiques, lorsque cela est possible; nous vous recommandons de ne permettre AUCUN port, AUCUN protocole.

Par exemple, une politique générée avec des restrictions de port et de protocole pourrait ressembler à ceci :

```
dst_ports {
 start_port: 22
 end_port: 22
 consumer_filters {
   application_name: "c:\\test\\putty.exe"
 }
}}
ip_protocol: TCP
```

En revanche, si vous autorisez les connexions réseau lancées par iperf.exe avec TOUS les protocoles et TOUS les ports, la politique générée ressemblera à ceci :

```
match_set {
  dst_ports {
    end_port: 65535
    consumer_filters {
      application_name: "c:\\test\\iperf.exe"
    }
  }
  address_family: IPv4
  inspection_point: EGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Pour le filtre ci-dessus, Cisco Secure Workload crée une règle de politique pour autoriser le trafic réseau sur le fournisseur comme suit :

```
match_set {
    dst_ports {
    end_port: 65535
  }
  address_family: IPv4
  inspection_point: INGRESS
  match_comment: "PolicyId=61008290755f027a92291b9d:61005f90497d4f47cedacb86:"
}
```

Cette règle de réseau ouvre tous les ports sur le fournisseur. Nous vous déconseillons de créer des filtres basés sur le système d'exploitation avec le protocole *Any* (Tous).

Configurer les politiques pour les attributs Windows

Pour plus de granularité lors de l'application d'une politique sur les charges de travail basées sur Windows, vous pouvez filtrer le trafic réseau par :

- Nom de l'application
- Nom du service
- Noms d'utilisateur avec ou sans groupes d'utilisateurs

Cette option est prise en charge dans les modes WAF et WFP. Les filtres basés sur le système d'exploitation Windows sont classés en tant que *filtres de consommateur* et de *filtres de fournisseur* dans la politique de réseau générée. Les filtres des consommateurs filtrent le trafic réseau qui est initié par la charge de travail des consommateurs et les filtres des fournisseurs filtrent le trafic réseau qui est destiné au travail du fournisseur.

Avant de commencer

Cette procédure suppose que vous modifiez une politique existante. Si vous n'avez pas encore créé la politique à laquelle ajouter un filtre basé sur le système d'exploitation Windows, créez d'abord cette politique.

Important Consultez Mises en garde, à la page 67 et Limites connues, à la page 66 pour des renseignements sur les politiques impliquant les attributs Windows.

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Defend (Défendre)** > **Segmentation** .

Étape 2 Cliquez sur la portée qui contient la politique pour laquelle vous souhaitez configurer des filtres basés sur le système d'exploitation Windows.

Étape 3 Cliquez sur l'espace de travail dans lequel vous souhaitez modifier la politique.

Étape 4 Cliquez sur **Manage Policies** (Gestion des politiques).

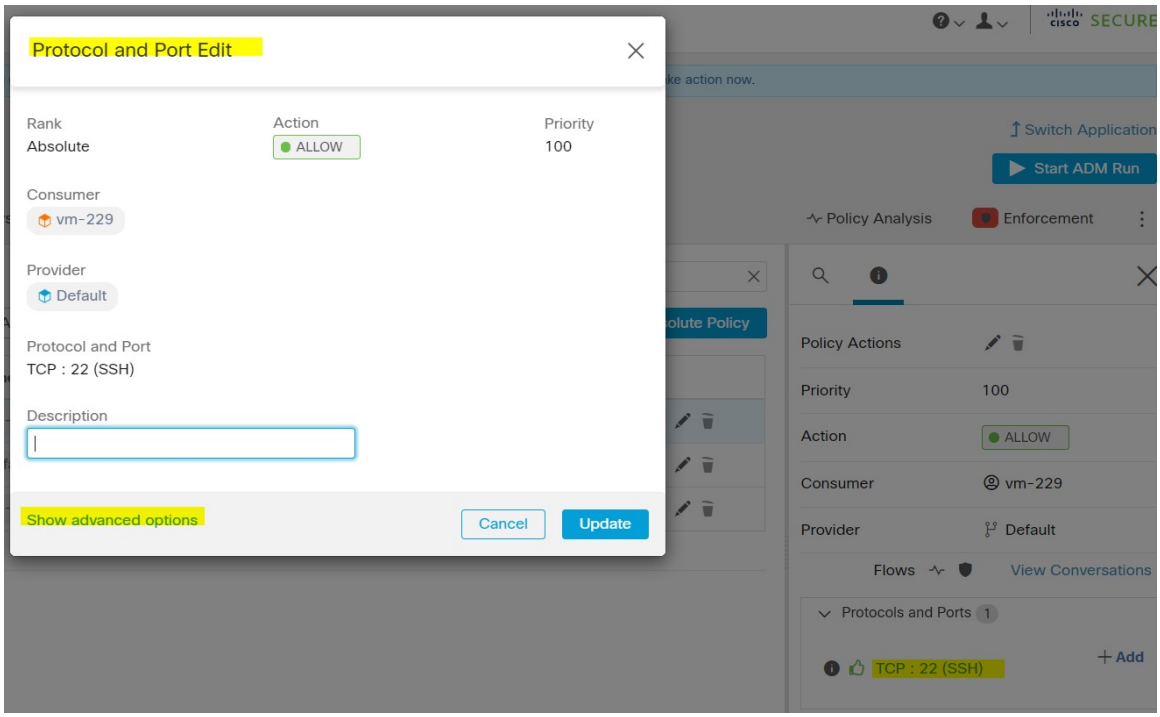
Étape 5 Choisissez la politique à modifier.

Important Le client et le fournisseur doivent inclure uniquement les charges de travail Windows.

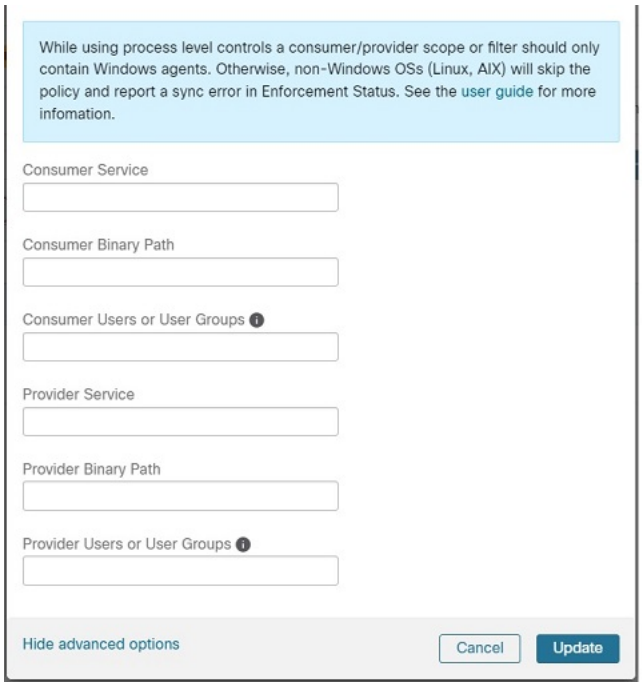
Étape 6 Dans la ligne du tableau permettant de modifier la politique, cliquez sur la valeur existante dans la colonne **Protocols and Ports** (protocoles et ports).

Étape 7 Dans le volet de droite, cliquez sur la valeur existante sous **Protocols and Ports**.

Dans l'exemple, cliquez sur **`TCP : 22 (SSH).`**



Étape 8 Cliquez sur **Show Advanced Options** (Afficher les options avancées).



Étape 9 Configurez les filtres de consommateur en fonction du nom de l'application, du nom du service ou du nom d'utilisateur.

- Le nom de l'application doit être un chemin d'accès complet.

- Le nom du service doit être un nom de service court.
- Le nom d'utilisateur peut être un nom d'utilisateur local (par exemple, tetter) ou un nom d'utilisateur de domaine (par exemple, capteur-dev@capteur-dev.com ou capteur-dev\capteur-dev)
- Le groupe d'utilisateurs peut être un groupe d'utilisateurs local (par exemple, Administrateurs) ou un groupe d'utilisateurs de domaine (par exemple, domaine utilisateurs\\capteur-dev)
- Plusieurs noms d'utilisateurs et/ou de groupes d'utilisateurs peuvent être spécifiés, séparés par « , » (par exemple, capteur-dev\@capteur-dev.com,utilisateurs du domaine\\capteur-dev)
- Le nom du service et le nom d’utilisateur ne peuvent pas être configurés ensemble.

Étape 10 Configurez les filtres de fournisseur en fonction du nom de l’application, du nom de service ou du nom d’utilisateur.

Suivez les mêmes directives que celles données à l’étape précédente pour les filtres du consommateur.

Étape 11 Saisissez les chemins d’accès au fichier binaire, le cas échéant.

Par exemple, saisissez **`c:\test\putty.exe`**

Étape 12 Cliquez sur **Update** (mettre à jour).

Limites connues

- Windows 2008 R2 ne prend pas en charge les politiques de filtrage basées sur le système d’exploitation Windows.
- La politique de réseau peut être configurée avec un nom d’utilisateur unique, tandis que l’interface utilisateur du pare-feu Microsoft prend en charge plusieurs utilisateurs.

Mises en garde

- Lors de l’utilisation de politiques basées sur le système d’exploitation Windows, une portée ou un filtre consommateur ou fournisseur ne doit contenir que des agents Windows. Sinon, les systèmes d’exploitation autres que Windows (Linux, AIX) ignorent la politique et signalent une erreur de synchronisation dans l’état d’application.
- Évitez de créer des filtres de système d’exploitation Windows avec des critères de filtrage *peu rigoureux*. De tels critères peuvent ouvrir des ports réseau indésirables.
- Si les filtres de système d’exploitation sont configurés pour le client, les politiques ne s’appliquent qu’au client. De même, s’ils sont configurés pour le fournisseur, ils ne s’appliquent qu’au fournisseur.
- Étant donné que les connaissances relatives au contexte du processus, de l’utilisateur ou de service sont limitées ou inexistantes, il y aura des écarts dans l’analyse des politiques si elles comportent des filtres basés sur le système d’exploitation Windows.

Vérification et dépannage des politiques avec les attributs de filtrage basés sur le système d’exploitation Windows

Si vous utilisez des attributs de filtrage basés sur le système d’exploitation Windows, les rubriques suivantes vous fourniront des informations de vérification et de dépannage.

Le service d'assistance Cisco TAC peut utiliser ces informations au besoin pour effectuer le dépannage de ces politiques.

Politiques basées sur le nom de l'application

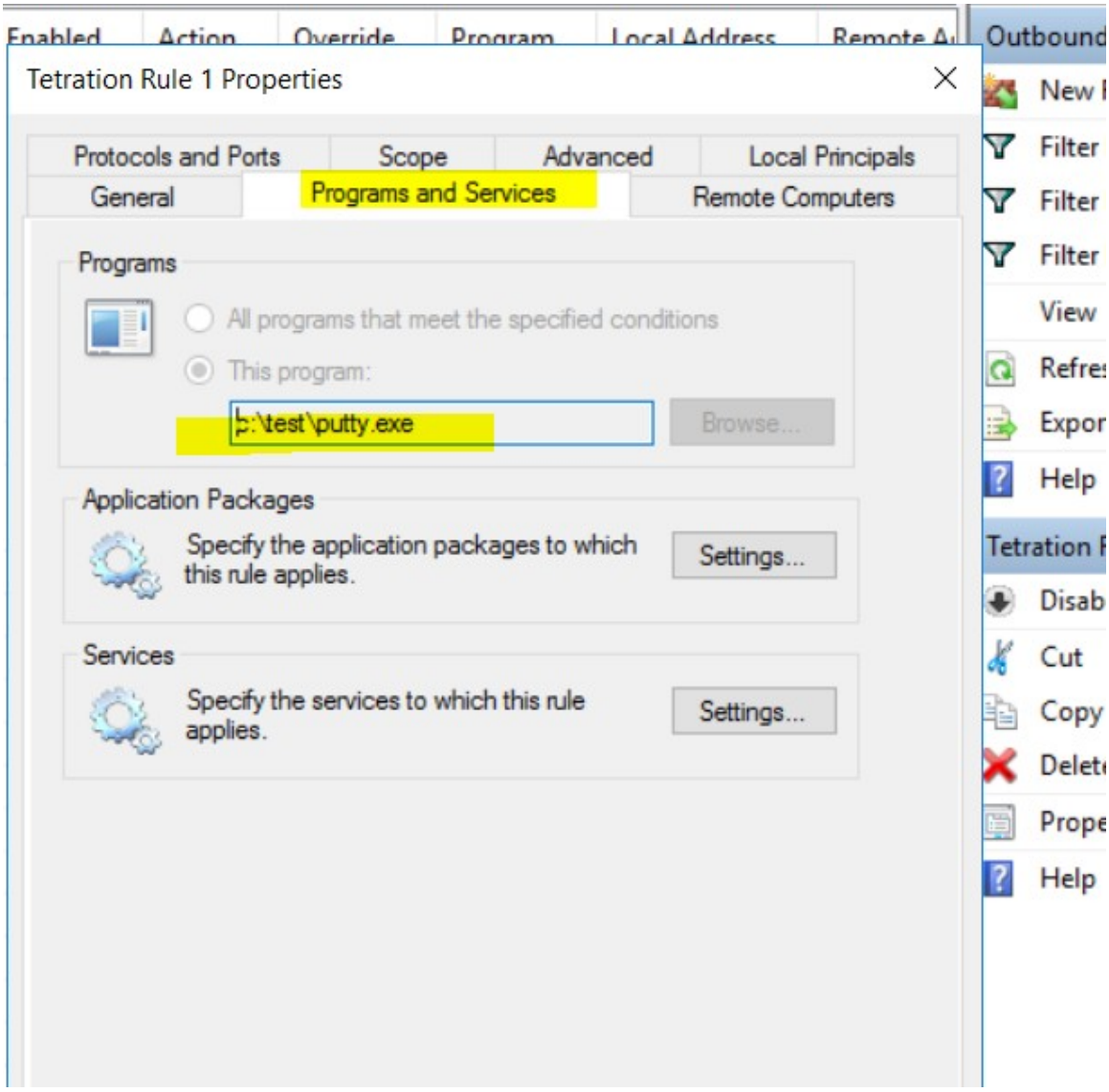
Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom de l'application sur les charges de travail avec système d'exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s'afficher sur la charge de travail pour un fichier binaire d'application saisi sous la forme **`c:\test\putty.exe`**.

Exemple de politique basée sur le nom de l'application

```
dst_ports {
start_port: 22
end_port: 22
consumer_filters {
application_name: "c:\test\putty.exe"
}
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier, à l'aide des outils Windows natifs, qu'un filtre a été ajouté à une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_APP_ID pour le nom de l'application dans le fichier de sortie : filter.xml.

```
<fieldKey>FWPM_CONDITION_ALE_APP_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
```

```
                              <type>FWP_BYTE_BLOB_TYPE</type>
                              <byteBlob>
                                     <data>
‹→5c006400650076006900630065005c006800610072006400640069007300 6b0076006f006
‹→</data>
                                  <asString>\device\harddiskvolume2\temp\putty.exe</
‹→asString>
                 </byteBlob>
       </conditionValue>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:                    Cisco Secure Workload Rule 1
----------------------------------------------------
EffectiveWeight:                18446744073709551592
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    22
Protocol:                       6
AppID:                          \device\harddiskvolume2\test\putty.exe
```

Nom d'application non valide

- En mode WAF, une règle de pare-feu est créée pour un nom d’application non valide.
- En mode WFP, le filtre WFP n’est pas créé pour un nom d’application non valide, mais le NPC n’est pas rejeté. L'agent consigne un message d'avertissement et configure le reste des règles de politique.

Politiques basées sur le nom du service

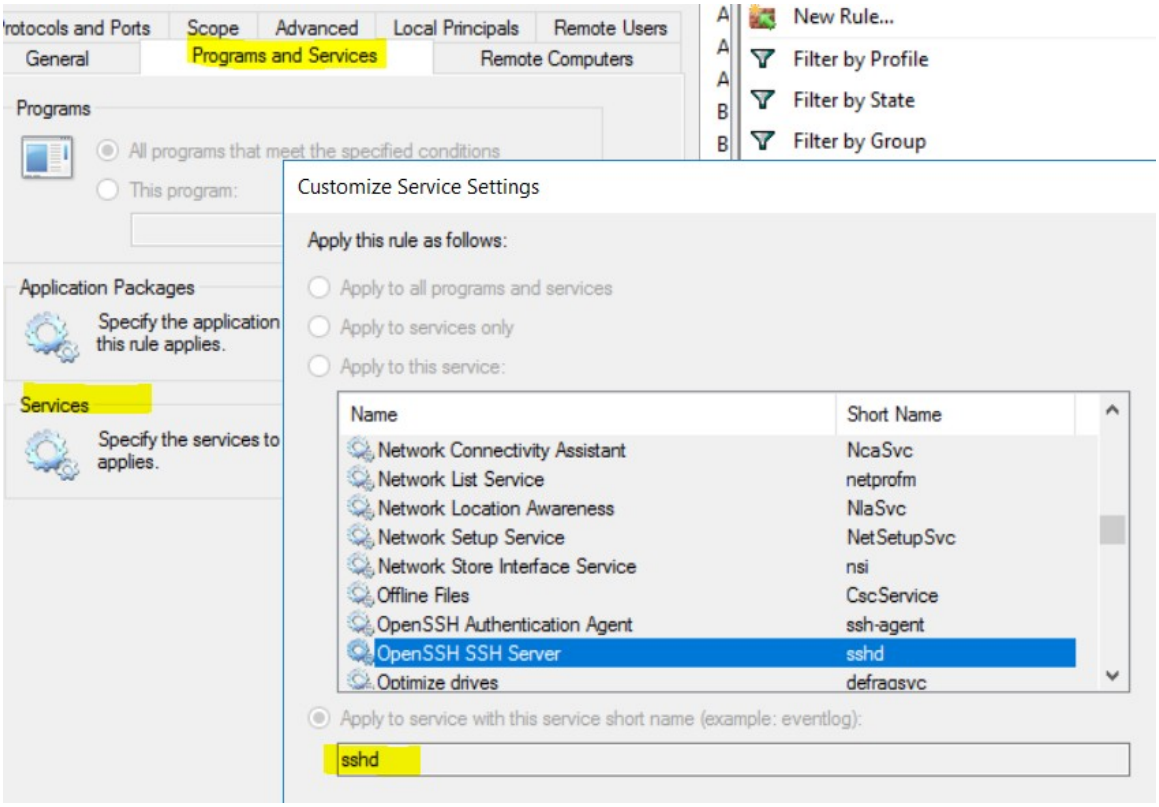
Utilisez les informations suivantes pour vérifier et dépanner les politiques basées sur le nom du service sur les charges de travail fonctionnant sous le système d’exploitation Windows.

Les sections suivantes décrivent la façon dont les politiques doivent s’afficher sur la charge de travail.

Exemple de politique basée sur le nom de service

```
    dst_ports {
             start_port: 22
             end_port: 22
             provider_filters {
                    service_name: “sshd”
             }
         }}
         ip_protocol: TCP
         address_family: IPv4
         inspection_point: INGRESS
```

Règle de pare-feu générée



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
                    <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
                    <matchType>FWP_MATCH_EQUAL</matchType>
                    <conditionValue>
                              <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>

<sd>O:SYG:SYD:(A;;CCRC;;;S-1-5-80-3847866527-469524349-687026318-
→516638107)</sd>
                    </conditionValue>
</item>
```

Filtre WFP généré à l'aide de tetenf.exe -l -f

```
Filter Name:       Cisco Secure Workload Rule 3
----------------------------------------------------
```

```
EffectiveWeight:            18446744073709551590
LayerKey:                   FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
Action:                     Permit
Local Port:                 22
Protocol:                   6
User or Service:            NT SERVICE\sshd
```

Nom non valide

- En mode WAF, la règle de pare-feu est créée pour un nom de service inexistant.
- En mode WFP, le filtre WFP n'est pas créé pour un nom de service inexistant.
- Le type de SID du service doit être *Unrestricted* (non restreint) ou *Restricted* (Restreint). Si le type de service est *None* (Aucun), la règle de pare-feu et le filtre WFP peuvent être ajoutés, mais n'ont aucun effet.

  Pour vérifier le type de SID, exécutez la commande suivante :

  ```
  sc qsidtype <service name>
  ```

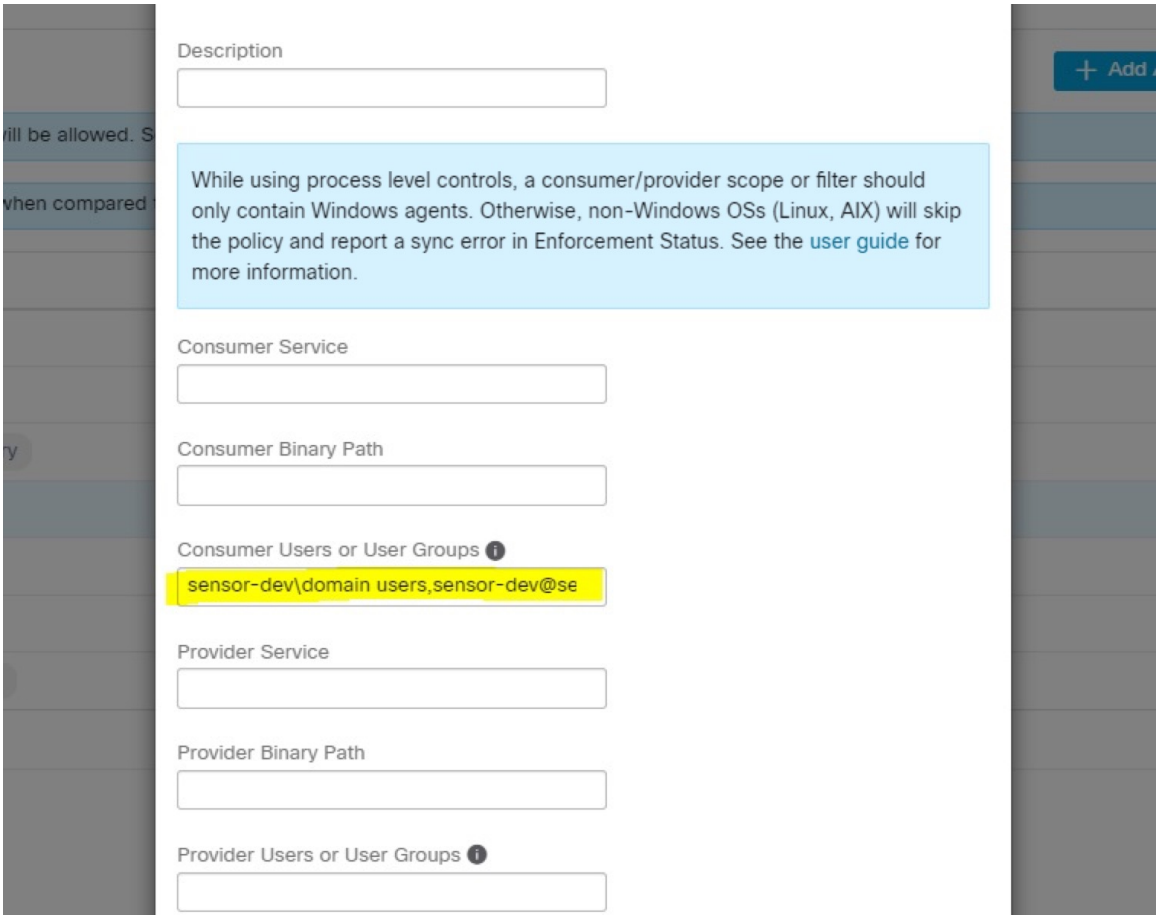
Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur

Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom d'utilisateur (avec et sans nom de groupe d'utilisateurs) sur les charges de travail avec système d'exploitation Windows.

Les sections de cette rubrique décrivent la manière dont les politiques doivent apparaître sur la charge de travail.

Les exemples présentés dans cette rubrique sont basés sur des politiques configurées avec les informations suivantes :

Figure 272: Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur



Exemple de politique basée sur le nom d'utilisateur

```
dst_ports {
          start_port: 30000
          end_port: 30000
          provider_filters {
               user_name: "sensor-dev\sensor-dev"
           }
}}
ip_protocol: TCP
address_family: IPv4
inspection_point: EGRESS
```

Exemple de politique basée sur le groupe d'utilisateurs et le nom d'utilisateur

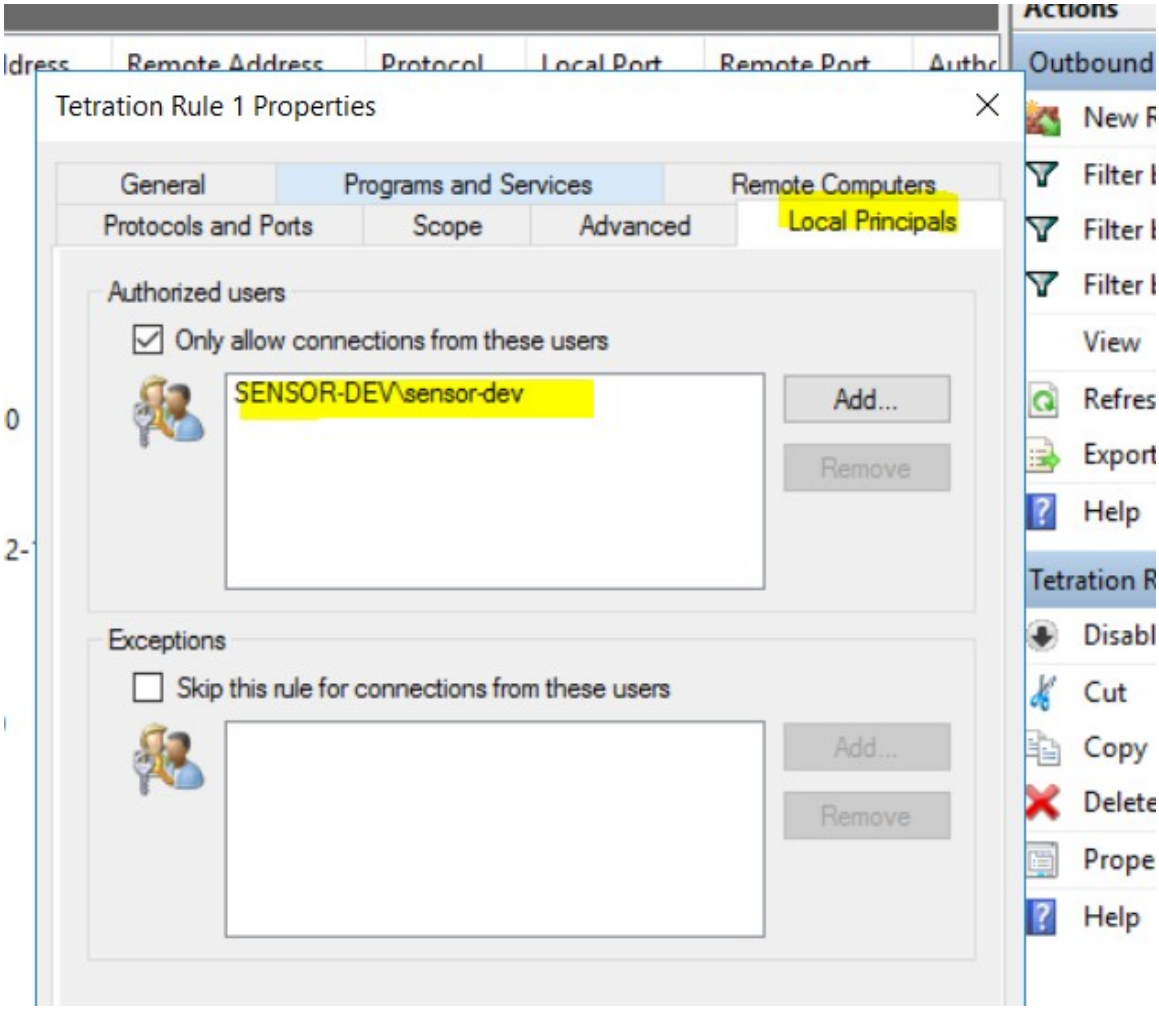
```
dst_ports {
start_port: 30000
end_port: 30000
provider_filters {
user_name: "sensor-dev\domain users,sensor-dev\sensor-dev"
}
}}
ip_protocol: TCP
```

```
address_family: IPv4
inspection_point: EGRESS
```

Règle de pare-feu générée

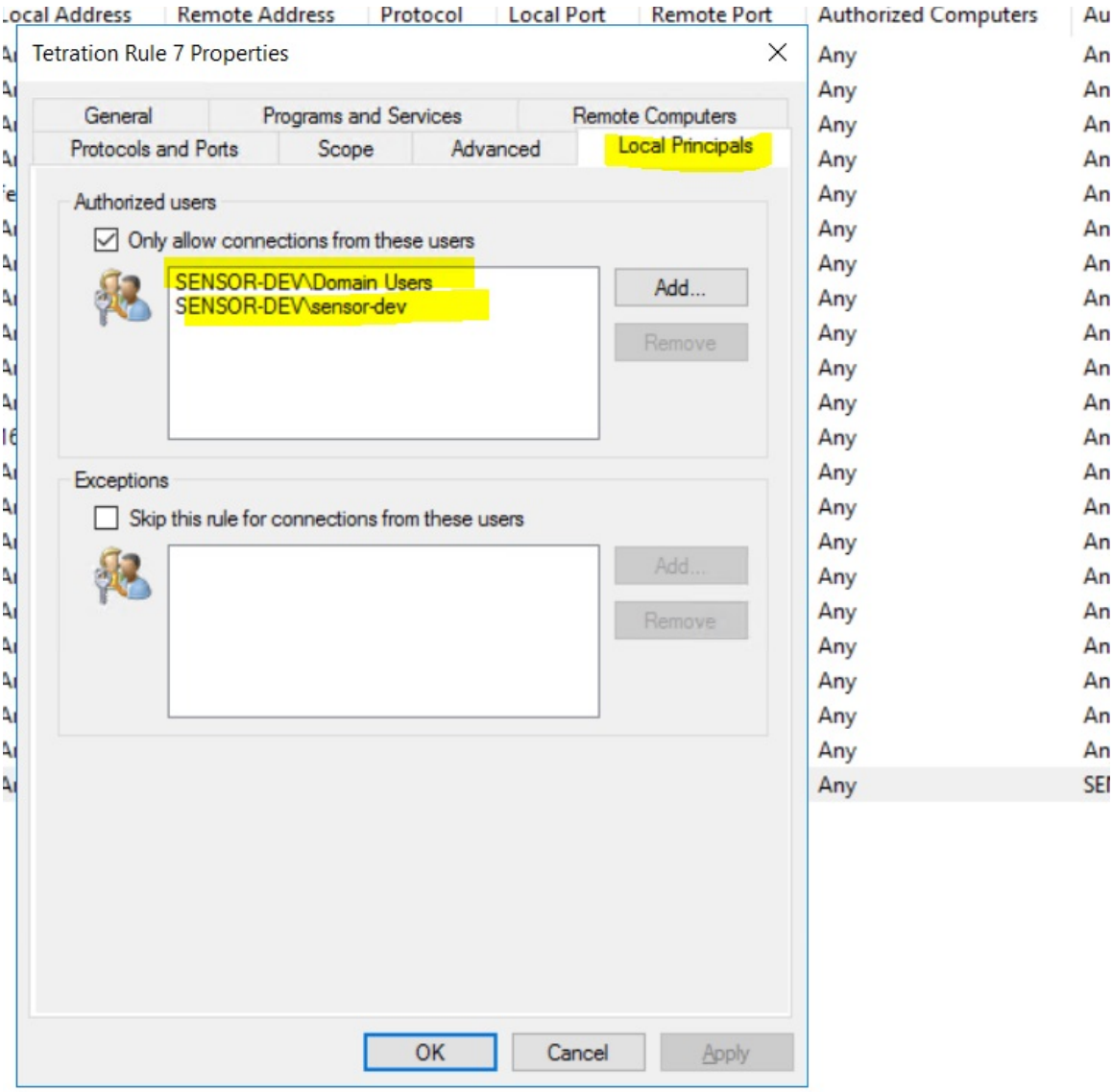
Règle de pare-feu basée sur le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\\sensor-dev



Règle de pare-feu basée sur le groupe d'utilisateurs et le nom d'utilisateur

Exemple : règle de pare-feu basée sur le nom d'utilisateur, sensor-dev\sensor-dev et le groupe d'utilisateurs, domain users\sensor-dev



Filtre généré à l'aide de netsh

Pour vérifier à l'aide des outils Windows natifs qu'un filtre a été ajouté pour une politique avancée :

- Avec des privilèges d'administration, exécutez `cmd.exe`.
- Exécutez `netsh wfp show filters`.
- Le fichier de sortie, **filter.xml**, est généré dans le répertoire actuel.
- Vérifiez FWPM_CONDITION_ALE_USER_ID pour déterminer le nom d'utilisateur dans le fichier de sortie : filter.xml.

```
<item>
            <fieldKey>FWPM_CONDITION_ALE_USER_ID</fieldKey>
            <matchType>FWP_MATCH_EQUAL</matchType>
            <conditionValue>
```

```
                    <type>FWP_SECURITY_DESCRIPTOR_TYPE</type>
                    <sd>O:LSD:(A;;CC;;;S-1-5-21-4172447896-825920244-2358685150)</sd>
                </conditionValue>
    </item>
```

Filtres WFP générés à l'aide de tetenf.exe -l -f

Filtrer en fonction du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\capteur-dev

```
Filter Name:                    Cisco Secure Workload Rule 1
----------------------------------------------------------
EffectiveWeight:                18446744073709551590
LayerKey:                       FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                         Permit
RemoteIP:                       10.195.210.15-10.195.210.15
Remote Port:                    30000
Protocol:                       6
User or Service:                SENSOR-DEV\sensor-dev
```

Filtrer en fonction du groupe d'utilisateurs et du nom d'utilisateur

Exemple : règle WFP basée sur le nom d'utilisateur, SENSOR-DEV\\sensor-dev et le nom du groupe d'utilisateurs, SENSOR-DEV\\Domain Users

```
Filter Name:         Cisco Secure Workload Rule 1
----------------------------------------------------
EffectiveWeight:             18446744073709551590
LayerKey:                    FWPM_LAYER_ALE_AUTH_CONNECT_V4
Action:                      Permit
RemoteIP:                    10.195.210.15-10.195.210.15
Remote Port:                 30000
Protocol:                    6
User or Service:             SENSOR-DEV\Domain Users, SENSOR-DEV\sensor-dev
```

Le nom du service et le nom d'utilisateur ne peuvent pas être configurés dans le cadre d'une règle de politiques réseau.

Note La politique réseau est rejetée par l'agent Windows si le nom d'utilisateur ou le groupe d'utilisateurs n'est pas valide.

Kubernetes et OpenShift

(Facultatif) Politiques supplémentaires pour les charges de travail Kubernetes

Les procédures suivantes sont facultatives, selon votre environnement Kubernetes.

Politiques pour le contrôleur d'entrée Nginx de Kubernetes fonctionnant en mode hôte-réseau

Cisco Secure Workload applique les politiques au niveau du contrôleur d'entrée nginx et au niveau des pods de arrière-plan lorsque ces derniers sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

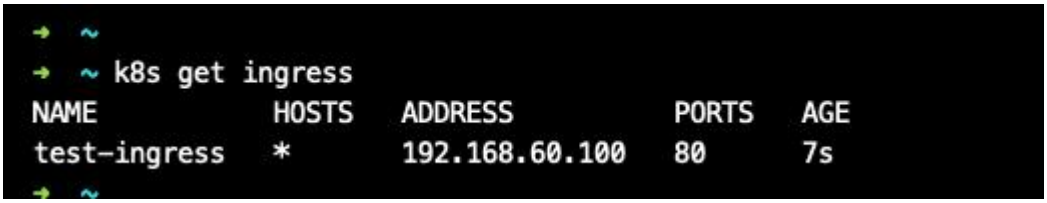
Note Si le contrôleur d'entrée ne fonctionne pas en mode réseau hôte, consultez IngressControllerAPI

Note IBM-ICP utilise le contrôleur d'entrée Nginx de Kubernetes par défaut et s'exécute sur les nœuds du plan de commande en mode réseau hôte.

Voici les étapes pour appliquer la politique à l'aide du contrôleur d'entrée Nginx Kubernetes.

Procedure

Étape 1 Créez un orchestrateur externe pour Kubernetes/OpenShift comme décrit ici.



Étape 2 Créez un objet d'entrée dans la grappe Kubernetes. Un instantané du fichier yaml utilisé pour créer l'objet d'entrée est fourni dans l'image suivante.

```
~
▶ k8s get ingress -o yaml
apiVersion: v1
items:
- apiVersion: extensions/v1beta1
  kind: Ingress
  metadata:
    annotations:
      virtual-server.f5.com/ip: 192.168.10.13
      virtual-server.f5.com/partition: k8scluster
    creationTimestamp: "2020-06-26T21:31:01Z"
    generation: 1
    labels:
      e2e-test: "yes"
    name: svc-ce2e-teeksitlbiwlc
    namespace: default
    resourceVersion: "1074475"
    selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/svc-ce2e-teeksitlbiwlc
    uid: 5526b4a3-b7f4-11ea-aa09-525400d58002
  spec:
    backend:
      serviceName: svc-ce2e-teeksitlbiwlc
      servicePort: 80
  status:
    loadBalancer:
      ingress:
      - ip: 192.168.10.13
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

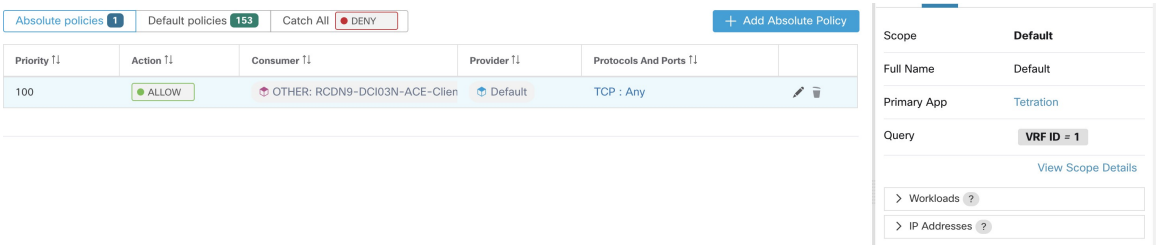
Étape 3 Déployez le contrôleur d'entrée Nginx de Kubernetes dans la grappe Kubernetes. Les pods du contrôleur d'entrée IBM-ICP s'exécutent sur les nœuds du plan de commande par défaut.

```
~
▶ k8s get pods -o wide -n ingress-nginx
NAME                                        READY   STATUS    RESTARTS   AGE     IP             NODE                          NOMINATED NODE
nginx-ingress-controller-6bc9c6745c-scfzs   1/1     Running   0          2m11s   192.168.10.13   enforcement-scale-16-kube3   <none>

~
▶ k8s get node enforcement-scale-16-kube3 -o wide
NAME                         STATUS   ROLES    AGE    VERSION   INTERNAL-IP     EXTERNAL-IP   OS-IMAGE            KERNEL-VERSION      CONTAINER-RUNTIME
enforcement-scale-16-kube3   Ready    <none>   7d5h   v1.12.3   192.168.10.13   <none>        Ubuntu 16.04.5 LTS   4.4.0-139-generic   docker://18.6.1
```

Étape 4 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accéderont. Dans l'exemple ci-dessous, nous avons créé un service simple *svc-ce2e-teeksitlbiwlc* (http-echo).

```
~
▶ k8s get svc svc-ce2e-teeksitlbiwlc
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
svc-ce2e-teeksitlbiwlc   ClusterIP   10.102.30.231   <none>        80/TCP    6m11s
```

Étape 5 Créez une politique entre le consommateur externe et le service backend.



Étape 6 Lorsque vous êtes prêt, appliquez la politique.

Étape 7 Dans le cas d'un contrôleur d'entrée Nginx, le logiciel Cisco Secure Workload applique la règle d'autorisation/abandon appropriée selon laquelle la source sera le consommateur spécifié à l'étape ci-dessus et la destination sera l'adresse IP du pod du contrôleur d'entrée correspondante. Dans le cas de pods backend, le logiciel Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le pod d'entrée et la destination sera l'adresse IP du pod backend (principal).

Politiques pour le contrôleur d'entrée de Kubernetes Nginx/Haproxy fonctionnant en tant que Déploiement/Daemonset

Cisco Secure Workload appliquera les politiques au contrôleur d'entrée et aux pods de l'arrière-plan (backend) lorsque les pods sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

Voici les étapes à suivre pour appliquer les politiques sur le contrôleur d'entrée.

Procedure

Étape 1 Créer ou mettre à jour un orchestrateur externe pour Kubernetes/OpenShift à l'aide d'OpenAPI. Consultez la section Orchestrateurspour en savoir plus sur la création de l'orchestrateur externe à l'aide d'OpenAPI. Ajoutez des informations sur les contrôleurs d'entrée pour la configuration de l'orchestrateur externe.

Étape 2 Créez un objet d'entrée dans la grappe Kubernetes.

Étape 3 Déployez le contrôleur d'entrée dans la grappe Kubernetes.

Étape 4 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accéderont.

Étape 5 Créez une politique entre le consommateur externe et le service backend.

Étape 6 Lorsque vous êtes prêt, appliquez la politique.

Étape 7 Dans le cas de contrôleurs d'entrée, Cisco Secure Workload le logiciel appliquera la règle d'autorisation/abandon appropriée selon laquelle la source sera le consommateur spécifié à l'étape ci-dessus et la destination sera l'adresse IP de pod du contrôleur d'entrée correspondante. Dans le cas de pods backend, le logiciel Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le pod d'entrée et la destination sera l'adresse IP du pod backend (principal).

Regroupement des charges de travail : grappes et filtres d'inventaire

Les grappes et les filtres d'inventaire ont des objectifs similaires, mais présentent des différences importantes :

Tableau 26 : Comparaison des grappes et des filtres d'inventaire

Grappes	Filtres d'inventaire
Sont utilisés pour appliquer une politique à un sous-ensemble des charges de travail dans une portée.	Peut être utilisé pour appliquer une politique à un sous-ensemble des charges de travail dans une portée. Peut également être utilisé pour appliquer une politique aux charges de travail, quelle que soit la portée (par exemple, pour appliquer une politique à toutes les charges de travail exécutant un système d'exploitation particulier).
Sont définis par une requête	Sont définis par une requête.
Peut inclure uniquement les charges de travail dans une seule portée.	L'adhésion peut être restreinte à une seule portée ou inclure des charges de travail de n'importe quelle portée (par exemple, si le filtre est basé sur le système d'exploitation).
Ne peut être utilisé que par les politiques du même espace de travail et de la même version de l'espace de travail.	Peut être utilisé par les politiques dans n'importe quelle portée et dans n'importe quel espace de travail.
Peut être créé automatiquement lors de la découverte automatique des politiques.	Doit être créé ou converti manuellement à partir d'une grappe existante.
Peut être remplacé lors de la découverte automatique des politiques s'il n'est pas approuvé. L'approbation de grappes connues intègres peut améliorer la précision d'autres grappes dans les futurs exécutions de découverte.	Ne sont jamais modifiés par la découverte automatique des politiques.
Profitez des fonctionnalités importantes de la découverte automatique des politiques. Il : • Disposer d'un indice de confiance qui vous aide à évaluer si les charges de travail du groupe doivent être regroupées. • Peuvent être comparées aux grappes générées lors d'autres exécutions de découverte de politiques sur le même espace de travail.	--
Ne peut pas être utilisée lors de la configuration de Dépendances externes, à la page 462 et des autres fonctionnalités liées aux politiques à portée croisée et à la découverte de politiques.	Peut être utilisé pour configurer des politiques granulaires impliquant des dépendances externes et d'autres fonctionnalités liées aux politiques à portée croisée, telles que les règles de pilote automatique.
Consultez Grappes, à la page 506 et les sous-sections.	Consultez les sections Créer un filtre d'inventaire, à la page 392 et Convertir une grappe en filtre d'inventaire, à la page 510.

Grappes

Une grappe est un ensemble de charges de travail qui sont regroupées dans un espace de travail. (Un déploiement Cisco Secure Workload peut également être appelé une grappe, mais les deux utilisations ne sont pas liées).

Par exemple, si la portée de votre application comprend plusieurs serveurs web parmi les nombreux autres types de serveurs et d'hôtes qui composent votre application, vous pourriez vouloir une grappe de serveurs web dans cette portée d'application, de sorte que vous puissiez attribuer des politiques spécifiques uniquement à ces serveurs web.

La découverte automatique des politiques regroupe les charges de travail en grappes en fonction des signaux observés pendant la période spécifiée lors de la configuration de l'exécution.

Chaque grappe est définie par une requête

Les requêtes de grappe sont dynamiques, sauf si vous les définissez avec des adresses IP spécifiques. Avec les requêtes dynamiques, les membres de la grappe peuvent changer au fil du temps pour refléter les modifications de votre inventaire : des charges de travail plus nombreuses, moins nombreuses ou différentes peuvent correspondre à la requête.

Par exemple, si une requête de grappe est basée sur un nom d'hôte contenant la sous-chaîne « RH ».

La découverte automatique des politiques examine les noms d'hôte et les étiquettes associés aux charges de travail. Pour chaque grappe, la découverte automatique des politiques génère une courte liste de requêtes candidates en fonction des noms d'hôte et de ces étiquettes. Parmi ces requêtes, vous pouvez en sélectionner une, éventuellement la modifier et l'associer à la grappe. Notez que, dans certains cas, lorsque la découverte automatique des politiques ne peut pas formuler de requêtes suffisamment simples en fonction des noms d'hôte et des étiquettes, aucune (autre) requête n'est suggérée.

Les charges de travail dans les grappes approuvées ne sont pas affectées par la découverte de politiques futures

Seules les charges de travail qui ne sont pas encore membres d'une grappe approuvée dans l'espace de travail approprié sont affectées par la découverte de politiques. Une **grappe approuvée** est une grappe que vous avez approuvée manuellement. Pour de plus amples renseignements, consultez la section Approbation des grappes, on page 514.

Modifier les grappes pour améliorer le regroupement

Dans les sections suivantes, nous décrivons quelques flux de travail pour modifier, améliorer et approuver les résultats de la mise en grappe. Notez que l'on ne peut modifier/approuver les grappes que dans la dernière version d'un espace de travail (voir Journaux d'activités et historique des versions).

Consultez Modification des grappes, on page 508.

Grappes concernant l'inventaire Kubernetes

Note Si votre espace de travail comprend l'inventaire de plusieurs espaces de noms Kubernetes, chaque requête de grappe doit être filtrée par espace de noms. Ajoutez le filtre d'espace de nom à chaque requête s'il n'est pas déjà présent. Si vous modifiez une requête, redécouvre automatiquement les politiques.

Une grappe peut comprendre une seule charge de travail.

Vous pouvez créer des politiques concernant une seule charge de travail.

Les grappes peuvent être converties en filtres d'inventaire

À l'instar des grappes approuvées, les grappes promues en filtres d'inventaire ne sont pas modifiées lors de la découverte ultérieure des politiques .

Contrairement aux grappes, les filtres d'inventaire ne sont pas liés à un espace de travail, mais sont disponibles globalement dans votre déploiement de Cisco Secure Workload.

Pour une comparaison des grappes et des filtres d'inventaire, consultez Regroupement des charges de travail : grappes et filtres d'inventaire, on page 504.

Consultez Convertir une grappe en filtre d'inventaire, on page 510.

Niveau de confiance de la grappe

Utiliser le niveau de confiance ou le niveau de qualité d'une grappe pour déterminer les grappes à améliorer.

Le niveau de confiance pour une grappe correspond à la moyenne des niveaux de confiance des charges de travail des membres. En général, plus une charge de travail est similaire aux autres membres de la grappe qui lui a été attribuée et plus elle est différente des charges de travail de la grappe alternative la plus proche (la plus similaire), plus la confiance en cette charge de travail est élevée.

Lorsque les flux sont utilisés pour le regroupement, deux charges de travail sont similaires lorsqu'elles ont un modèle de conversation similaire (comme des ensembles similaires de voisins dans le graphe de conversation, c'est-à-dire des ensembles similaires de charges de travail et de ports de consommateurs et de fournisseurs).

Note

- Le niveau de confiance des grappes n'est pas calculé (est indéfini) pour :
  - les grappes contenant une seule charge de travail
  - les grappes approuvées
  - les charges de travail de la portée pour lesquelles aucune communication n'a été observée (ou aucune information sur les processus n'est disponible, si le regroupement basé sur les processus a été choisi)
- Les grappes ne dépassent pas les limites de la partition (comme les limites de sous-réseau, reportez-vous aux étiquettes de routage des configurations de découverte automatique de politiques avancées). Cependant, dans le calcul de la confiance et de la grappe de secours, ces limites sont ignorées. Cela indique l'existence potentielle de charges de travail ou de grappes qui se comportent de manière très similaire, même si elles se trouvent dans des sous-réseaux différents.
- Après la modification des grappes, les niveaux de confiance peuvent devenir inexacts, car ils ne sont PAS recalculés avant que vous ne détectiez à nouveau les politiques.

Pour afficher le niveau de confiance de la grappe, voir Afficher les grappes, on page 507.

Afficher les grappes

La vue des grappes prend en charge l'association requête à grappe et la modification des requêtes.

Dans la vue des grappes, vous pouvez cliquer sur un en-tête de colonne du tableau pour trier les grappes en fonction de cette colonne (comme le nom, le nombre de charges de travail ou le niveau de confiance).

Pour chaque grappe, en cliquant sur la ligne, vous pouvez afficher d'autres informations sur la grappe, telles que la description, les requêtes suggérées ou approuvées, et les charges de travail des membres dans le panneau de droite. Plusieurs de ces champs sont modifiables.

Pour afficher les grappes et leurs détails :

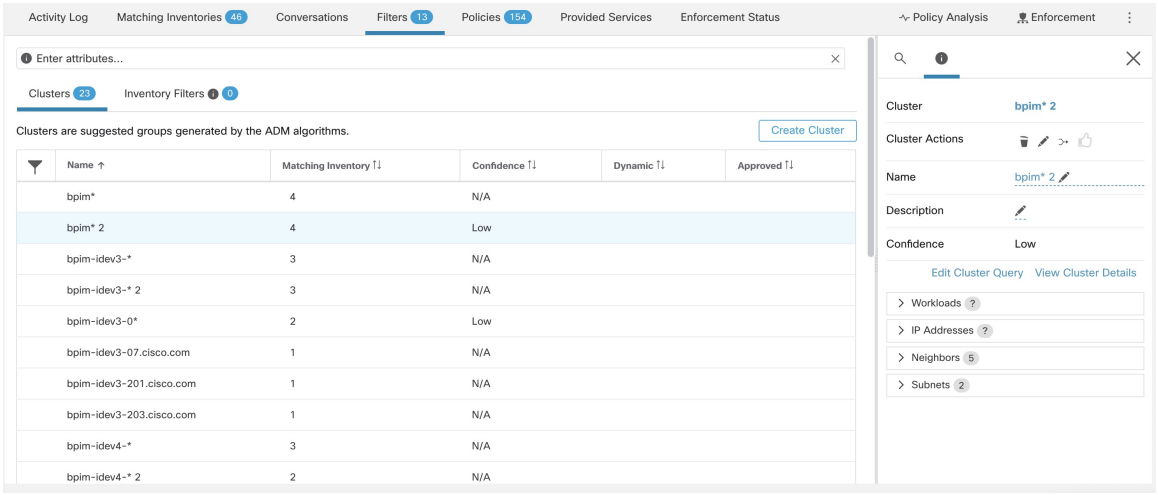
1. Accédez à la portée et à l'espace de travail qui vous intéressent.

   Les grappes sont spécifiques à un espace de travail; chaque espace de travail d'une portée peut avoir des grappes différentes. Pour rendre les grappes disponibles en dehors de leur espace de travail actuel, consultez Convertir une grappe en filtre d'inventaire, on page 510.

2. Cliquez sur **Manage Policies** (Gestion des politiques).
3. Cliquez sur **Filters** (Filtres).
4. Cliquez sur **Clusters** (Grappes).
5. Pour afficher des informations sur une grappe, cliquez sur cette dernière.
   a. Regardez dans le panneau qui s'ouvre sur la droite.
   b. Pour en savoir plus, cliquez sur **View cluster Details**(Afficher les détails de la grappe) .

      La page Cluster Details (détails de la grappe) s'ouvre dans un onglet de navigateur distinct.

Figure 273: Affichage des grappes



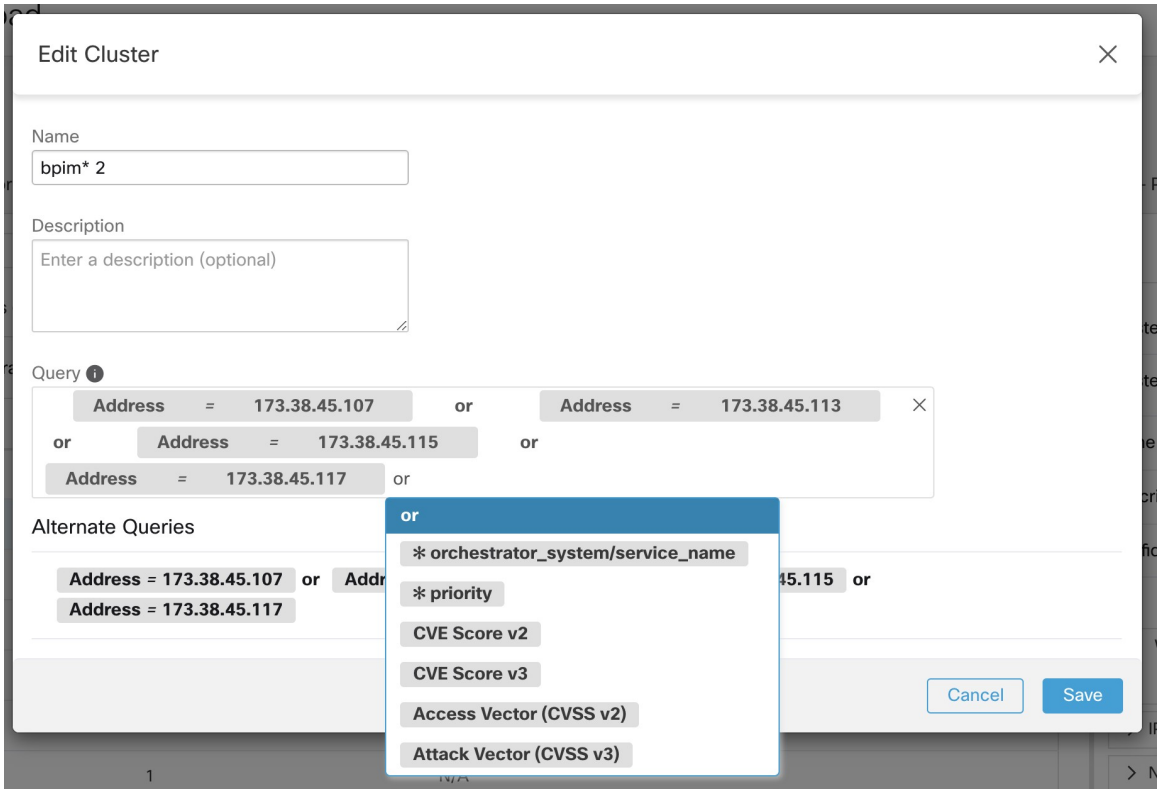
Modification des grappes

La découverte automatique des politiques crée une ou plusieurs requêtes candidate pour chaque grappe.

Si les résultats de la mise en grappe ne correspondent pas complètement à vos attentes, vous pouvez améliorer cette dernière en modifiant la requête.

Pour parcourir et modifier des grappes : Cliquez sur la zone **clusters** (grappes) en haut de la page. Pour modifier une grappe (p. ex., modifier les membres d'une grappe ou sélectionner/modifier sa requête), sélectionnez/modifiez la requête de la grappe, comme indiqué ci-dessous.

Figure 274: Modifier la grappe



Vous pouvez ajouter ou supprimer des adresses IP explicites, ou choisir une autre requête dans la liste d'alternatives fournie et modifier cette requête. La requête d'une grappe peut correspondre à n'importe quel filtre de requête exprimé en termes d'adresses, de noms d'hôte et d'étiquettes. Si vous définissez une requête basée sur des étiquettes plutôt que sur des adresses IP explicites, la grappe sera dynamique et un inventaire nouveau, modifié ou supprimé qui est correctement étiqueté sera automatiquement inclus ou exclu de la grappe.

Une fois la sélection de la requête et les modifications possibles terminées, cliquez sur Save (enregistrer). Notez qu'une fois que vous avez cliqué sur le bouton SAVE, la grappe est automatiquement marquée comme approuvée et l'icône représentant un pouce levé devient bleu (qu'une modification ait été apportée ou non). L'icône d'approbation peut être alternée pour modifier le statut d'approbation comme vous le souhaitez. Pour en savoir plus, reportez-vous à Approbation des grappes, on page 514

Important Lorsque l'appartenance à une grappe est modifiée, il peut être nécessaire de découvrir à nouveau les politiques pour obtenir une politique mise à jour reflétant avec précision les modifications des flux entre les grappes modifiées. En effet, les appartenances aux grappes peuvent avoir changé (par exemple, de nouveaux nœuds ont été ajoutés à une grappe). Une situation similaire peut se produire si la portée correspondant à l'espace de travail est modifiée ou, de manière générale, lorsque l'appartenance à l'espace de travail change. De même, les niveaux de confiance des grappes peuvent ne plus être précis selon les modifications apportées aux adhésions aux grappes. Dans tous ces cas, la nouvelle découverte automatique des politiques est utile pour obtenir des politiques et des niveaux de confiance des grappes à jour (niveau de confiance mis à jour sur les grappes non approuvées).

Si vous modifiez des requêtes de grappe, il est possible que les grappes associées aux requêtes se chevauchent.

Convertir une grappe en filtre d'inventaire

Convertir une grappe en filtre d'inventaire si :

- Vous ne souhaitez pas que la grappe soit modifiée par les futures exécutions de découverte automatique de la politique, ce qui constitue une alternative plus souple à l'approbation de la grappe.
- Vous souhaitez que la grappe soit indépendante de l'espace de travail et dans la version de l'espace de travail.
- Vous créez ou découvrez des politiques dans lesquelles le consommateur et le fournisseur appartiennent à des portées différentes, et vous souhaitez créer des politiques spécifiques à un sous-ensemble de charges de travail dans une portée, pas seulement des politiques impliquant la portée entière.

  Vous devez utiliser des filtres d'inventaire plutôt que des grappes à cette fin si vous créez des politiques concernant plusieurs portées à l'aide de la méthode avancée décrite en Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 522 et que vous souhaitez que les politiques soient plus appliquées plus finement que de portée à portée.

Procédure

Étape 1 Accédez à l'espace de travail qui contient la grappe à promouvoir.

Étape 2 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 3 Cliquez sur **Filters** (Filtres).

Étape 4 Cliquez sur **Clusters** (Grappes).

Étape 5 Cliquez sur la grappe que vous souhaitez utiliser dans la politique multiportée.

Étape 6 Dans le panneau de droite, dans la section **Cluster Actions** (Actions de niveau grappe), cliquez sur (Promote to Inventory Filter)(Promouvoir en tant que filtre d'inventaire).

Étape 7 Vérifiez que le nom, la description et la requête sont conformes aux attentes.

Étape 8 Sélectionnez **Restrict Query to Ownership Scope** Restreindre la requête au propriétaire de la portée)..

(Les filtres d'inventaire peuvent dépasser les limites de la portée, mais ce n'est pas ce que vous recherchez; vous souhaitez que ce filtre n'inclue que les charges de travail de cette portée).

Étape 9 Si vous souhaitez que l'application définie par ce filtre d'inventaire soit le fournisseur dans les politiques générées lors de la découverte automatique des politiques, sélectionnez **Provides a service external of its scope** (Fournit un service externe à sa portée).

Si cette application est un consommateur plutôt qu'un fournisseur, ou si vous utilisez ce filtre d'inventaire uniquement pour les politiques créées manuellement, vous n'avez pas besoin d'activer cette option.

Étape 10 Cliquez sur **Promote Cluster** (Promouvoir la grappe).

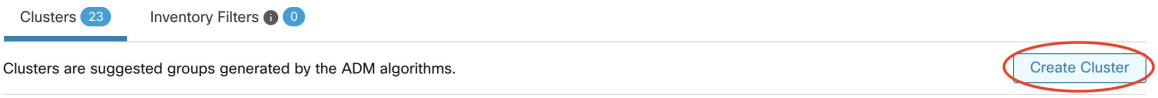
Étape 11 Vérifiez que la grappe a été déplacée vers l'onglet **Inventory Filters** (filtres d'inventaire).

Vous devrez peut-être actualiser la page pour constater ce changement.

Création ou suppression des grappes

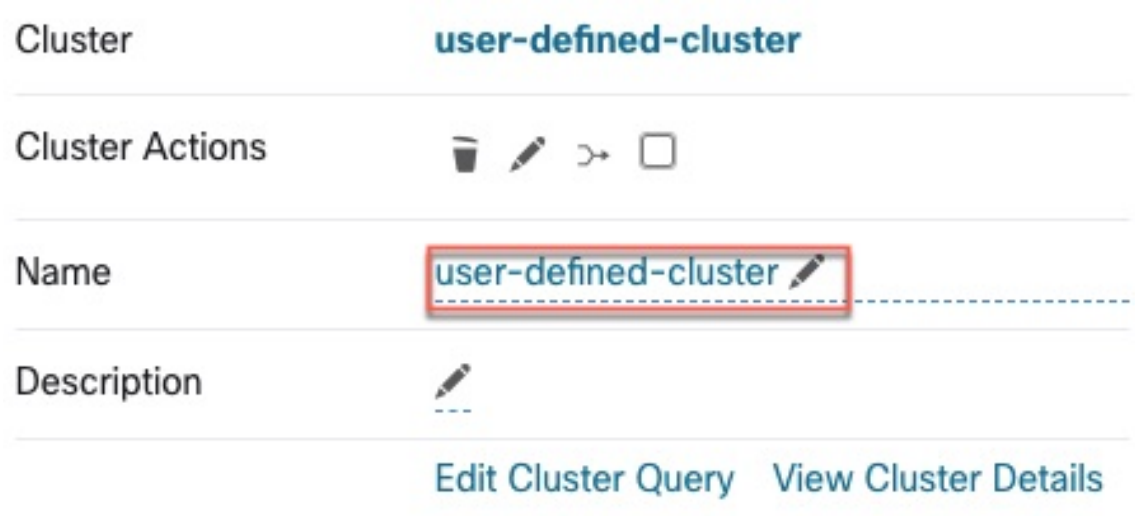
Cliquez sur le bouton **Create Cluster** (créer une grappe) dans la page des grappes pour créer une nouvelle grappe vide. Vous pouvez également créer une grappe à partir de la page de découverte automatique des politiques en cliquant sur le bouton **Create Filter** (Créer un filtre) dans la barre latérale de démarrage et en sélectionnant Grappes dans la boîte de dialogue modale.

Figure 275: Création d'une nouvelle grappe



La nouvelle grappe définie par l'utilisateur s'affichera dans le panneau latéral pour être renommée, si nécessaire.

Figure 276: Changement de nom d'une grappe



Une grappe vide peut être supprimée en la sélectionnant dans l'une des vues afin que les détails s'affichent dans le panneau latéral, puis en cliquant sur la corbeille dans l'en-tête de la vue détaillée de la grappe. Voir la figure ci-dessus.

Comparaison des versions des grappes générées : vues des différences

Après avoir détecté automatiquement au moins deux fois les politiques pour un espace de travail, vous pouvez comparer les grappes générées dans différents cycles de découverte.

Procedure

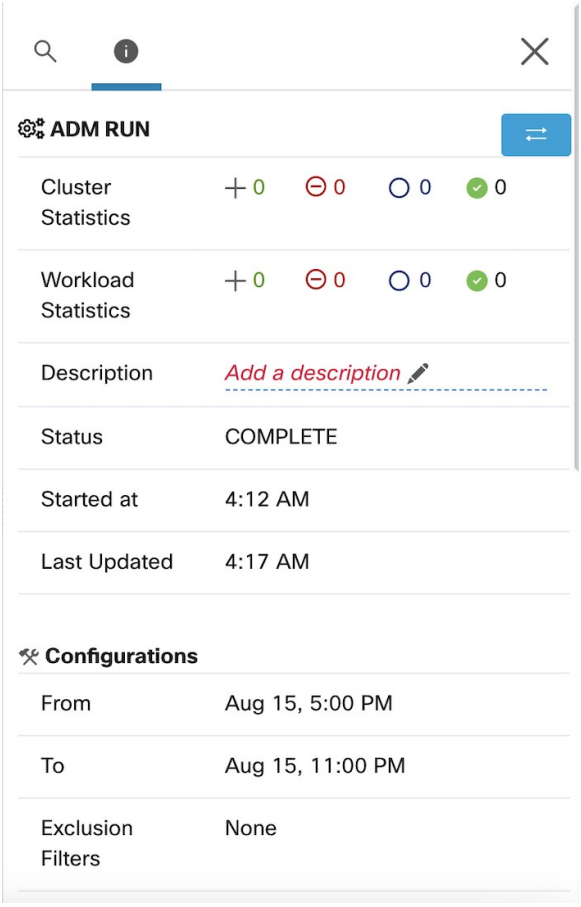
Étape 1 Accédez à la vue diff des grappes en utilisant l'un des chemins suivants :

- Après la découverte des politiques avec succès, un message s'affichera pour indiquer la réussite avec un lien qui mène à la vue du diff affichant les résultats de la découverte. Cliquez sur le lien des résultats.

Figure 277: Exécution réussie de la découverte automatique des politiques

- Comparer les révisions à partir de la vue des versions :
  a. Suivez les étapes dans Afficher, comparer et gérer les versions de politiques découvertes, on page 483.
  b. Après avoir cliqué sur **Compare Revisions** (Comparer les révisions), cliquez sur **Clusters** (Grappes).
- Dans le panneau latéral des détails dans la version :
  a. Suivez les étapes pour afficher les détails dans la version dans Afficher, comparer et gérer les versions de politiques découvertes, on page 483.
  b. Lorsque le panneau latéral affiche les informations contextuelles d'un cycle de découverte automatique des politiques, cliquez sur le bouton à double flèche situé dans le coin supérieur droit de ce panneau :

Figure 278: Affichage des informations de contexte



Étape 2 Choisissez les versions à comparer.

Étape 3 Passez en revue les résultats de la comparaison :

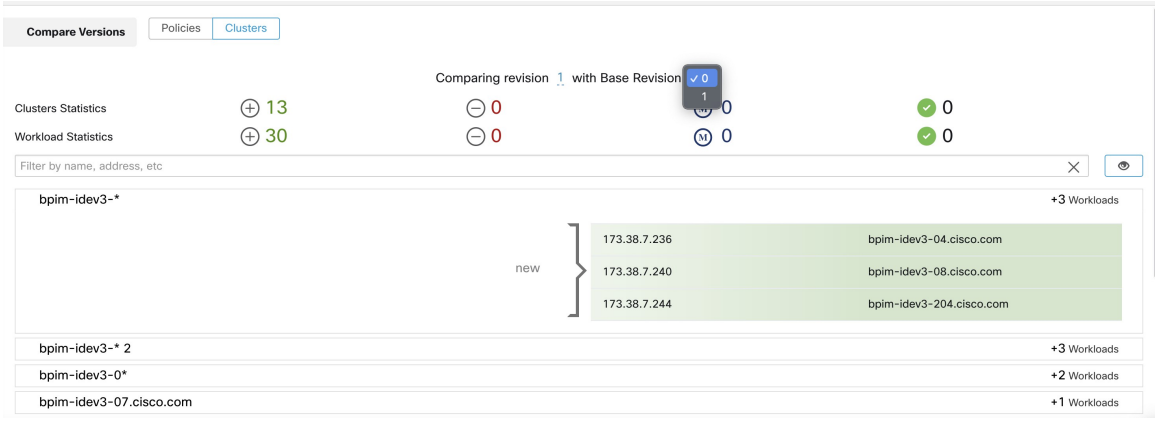
Au niveau supérieur, la vue Diff pour les politiques détectées automatiquement présente des statistiques générales sur les modifications apportées aux grappes et aux charges de travail en indiquant le nombre de grappes et de charges de travail ajoutées, supprimées, modifiées et inchangées.

Le reste de la vue est organisé sous forme de liste de groupes dans l'ordre d'ajout, de suppression, de modification et de changement, chaque couleur étant codée pour refléter l'état ainsi que le nombre de charges de travail ajoutées ou supprimées de la grappe.

Vous pouvez rechercher un groupe ou une charge de travail en particulier par son nom ou son adresse IP. Pour voir comment le contenu d'une grappe a changé, cliquez sur l'une des lignes représentant une grappe pour développer cette ligne.

Note Par défaut, les grappes inchangées sont masquées. Pour afficher les grappes inchangées, cliquez sur le bouton avec l'icône en forme d'œil.

Figure 279: Vue des différences de la grappe



What to do next

Pour afficher une comparaison similaire pour les politiques, consultez Comparaison des versions des politiques : différence de politique.

Prévention de la modification des grappes lors des réexécutions de découverte automatique des politiques

Si vous ne souhaitez pas que la découverte automatique des politiques (anciennement ADM) modifie une grappe lorsque vous découvrirez automatiquement les politiques de l'espace de travail à l'avenir, approuvez la grappe.

Par exemple, approuvez la grappe si vous avez modifié la requête de grappe et que vous devez maintenant ajouter de nouvelles charges de travail à la portée et les regrouper sans affecter les politiques existantes. L'approbation de la grappe fige le contenu et les attributs de la grappe dans l'état actuel. La découverte automatique des politiques ne modifie pas les grappes approuvées.

Consultez Approbation des grappes, à la page 514.

Sinon, vous pouvez promouvoir la grappe en tant que filtre d'inventaire, qui ne sera jamais modifié par la découverte de politiques. Consultez Convertir une grappe en filtre d'inventaire, à la page 510.

Approbation des grappes

Note Consultez également Convertir une grappe en filtre d'inventaire, on page 510, qui peut être une option plus appropriée pour vos besoins.

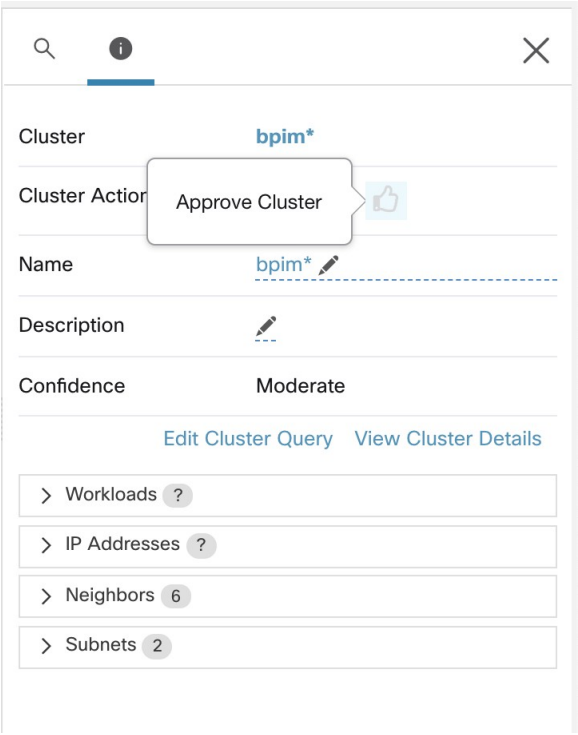
Après avoir approuvé une grappe, la découverte automatique ultérieure des politiques ne modifie pas la requête de cette grappe. Les adhésions aux grappes approuvées ne peuvent changer que si les membres de l'espace de travail changent.

Les charges de travail qui sont membres d'une grappe approuvée peuvent être appelées « charges de travail approuvées ».

Pour approuver une grappe :

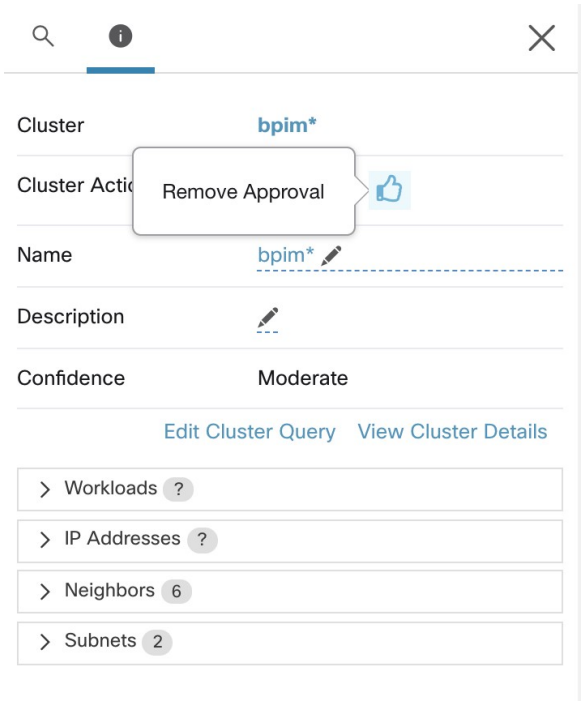
Vérifiez que la grappe qui vous intéresse est affichée sur le panneau latéral. Pour ce faire, vous devez rechercher la grappe ou cliquer sur la grappe souhaitée sur le tableau dans l'un des affichages. Ensuite, cochez la case dans le coin supérieur droit des informations de grappe sur le panneau latéral, comme illustré ci-dessous. Une fois qu'une grappe est approuvée, elle indique qu'elle restera inchangée par la future découverte automatique de politiques.

Figure 280: Approbation des grappes



Pour supprimer l'approbation d'une grappe, cliquez sur l'icône d'approbation .

Figure 281: Suppression de l'approbation d'une grappe



Aborder les complexités de la politique

Les résultats de l'application sont concernés par des facteurs tels que les éléments suivants :

- Type et rang de règle :
  - Politiques absolues et politiques par défaut
  - Le paramètre collecteur 'catch-all) pour l'espace de travail

  Consultez Rang de politique : Absolue, Par défaut et Collectrice, à la page 437.
- Ordre des politiques dans l'espace de travail

  Consultez Priorités des politiques, à la page 516.
- politiques héritées des portées parents ou ancêtres, y compris la règle « collectrice »

  Vous devez vous assurer qu'une politique de priorité plus élevée n'atteint pas de trafic avant la politique qui est censée atteindre ce trafic.

  Pour connaître les incidences des politiques dans les portées ascendantes, exécutez une analyse en direct des politiques sur toutes les portées concernées. Consultez Analyse des politiques en temps réel, à la page 546.

  Lorsque vous êtes prêt à appliquer les politiques d'un espace de travail, un assistant vous indique quelles politiques héritées ont une incidence sur les charges de travail dans l'espace de travail. Pour en savoir plus, consultez Assistant d'application des politiques, à la page 564.
- Interactions avec les politiques entre portées

(Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes ou qu'une extrémité de la conversation se trouve dans une portée différente de celle de la politique)

Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 522.

- Situations dans lesquelles le consommateur ou le fournisseur réel dans une politique peut différer des consommateurs et fournisseur configurés par défaut, par exemple dans des scénarios de basculement.

  Consultez Consommateur ou fournisseur réel, à la page 535.

Priorités des politiques

Le traitement du trafic est affecté par :

- La priorité des politiques dans la portée; et
- Ordre global des politiques et résolution des conflits, on page 516

les priorités des politiques dans une portée

Dans un espace de travail, l'ordre des politiques dans la liste reflète la priorité relative de chaque politique, la politique de priorité la plus élevée en haut de la liste et la politique de priorité la plus faible en bas de la liste.

Dans chaque espace de travail, les politiques absolues ont priorité sur les politiques par défaut, et la politique Collectrice est la politique de priorité la plus basse de l'espace de travail.

Pour de plus amples renseignements, consultez la section Rang de politique : Absolue, Par défaut et Collectrice, on page 437.

Ordre global des politiques et résolution des conflits

Des conflits peuvent survenir entre différentes politiques définies dans différentes portées. Plus précisément, des conflits surviennent pour les charges de travail (éléments de l'inventaire) qui appartiennent à plusieurs portées, comme parent/enfant, lorsque ces portées ont des politiques contradictoires).

Il n'est pas possible de résoudre ces conflits manuellement en raison de la nature dynamique de l'appartenance à la portée; les charges de travail peuvent entrer et sortir de la portée à mesure que leurs propriétés changent. Par conséquent, le système applique un ordre global à toutes les politiques, comme décrit ci-dessous, en fonction de la portée dans laquelle elles sont définies. Pour chaque charge de travail, la liste des politiques pertinentes (selon le consommateur/fournisseur/portée) est identifiée et triée par ordre global. La décision d'autoriser ou d'abandonner un flux est prise en fonction de la *première* politique correspondante de la liste triée.

En comprenant le schéma d'ordre général des politiques de sécurité, les administrateurs réseau peuvent définir les portées correctes et leurs priorités pour appliquer l'ensemble des politiques souhaitées sur les charges de travail. Dans chaque portée, les propriétaires d'applications conservent la capacité d'appliquer des politiques précises sur leurs charges de travail respectives.

Une politique de réseau global présente les caractéristiques suivantes :

- Un ensemble de portées classées par priorité (priorité la plus élevée en premier).
- L'espace de travail principal de chaque portée comporte des politiques absolues, des politiques par défaut et une action collectrice (catch-all) globale.

- Chaque groupe de politiques absolues ou par défaut de chaque espace de travail est trié en fonction de ses priorités locales (la plus élevée en premier).

L'ordre global des politiques est défini comme suit :

- Groupes de politiques absolues des espaces de travail principaux de toutes les portées (classés de la priorité la plus élevée à la plus faible).
- Groupes de politiques par défaut de l'espace de travail principal, toutes les portées (classés de la priorité la plus basse à la plus élevée).
- Politiques collectrices globales de toutes les portées (classées de la priorité la plus basse à la plus élevée).

Notez que l'ordre de portée s'applique aux groupes de politiques des catégories 1 et 2 plutôt qu'aux politiques individuelles. Dans chaque groupe, les politiques individuelles ayant des numéros de priorité de politiques inférieurs prévalent.

Pour une charge de travail spécifique, le sous-ensemble de portées auquel elle appartient est déterminé, puis l'ordre ci-dessus est appliqué. La politique globale de l'espace de travail de priorité la plus basse (appliquée) auquel cette charge de travail appartient est la règle collectrice applicable (mais une politique absolue ou par défaut peut la remplacer). Pour un flux donné sur cette charge de travail, l'action de la politique de correspondance la plus élevée est appliquée.

Note

- Si un espace de travail n'a ni politique absolue ni politique par défaut définies, il est ignoré. La politique collectrice globale de l'espace de travail ne sera pas incluse dans l'ordre global.
- L'ordre des politiques par défaut dans l'ordre global est inversé par rapport aux priorités de la portée. Cela vous permet de définir des politiques générales pour toutes les portées afin de sécuriser le périmètre de tous les espaces de travail, y compris ceux pour lesquels l'application des politiques n'est pas activée. Dans le même temps, les propriétaires d'applications qui ont activé la mise en application sur leur portée ont la possibilité de remplacer ces politiques par défaut.
- Le chevauchement des portées n'est pas recommandé. Consultez Chevauchement de portée, on page 370 pour en savoir plus. Toutefois, si une charge de travail comporte au moins deux interfaces, dans des portées qui se chevauchent ou disjointes, la politique collectrice catch-all de l'espace de travail de priorité le plus bas pour laquelle la mise en application est activée s'appliquera (parmi toutes les politiques collectrices applicables).

Nous développons notre exemple précédent à trois portées pour illustrer ce schéma de commande. Supposons que les priorités suivantes sont attribuées aux trois portées Utiliser des espaces de travail pour gérer les politiques pour obtenir des instructions sur la façon de modifier les priorités de portées) :

1. Applis
2. Applis RH
3. Applis Commerce

L'espace de travail principal de chacune de ces portées comporte des politiques absolues, des politiques par défaut et une action collectrice. Chaque groupe de politiques absolues ou par défaut de chaque espace de travail est trié en fonction de ses priorités locales.

L'ordre global des politiques est le suivant :

1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques absolues Applis Commerce
4. Politiques par défaut Applis Commerce
5. Politiques par défaut Applis RH
6. Politiques par défaut Applis
7. Politique collectrice Applis Commerce
8. Politique collectrice Applis RH
9. Politique collectrice Applis

Une charge de travail qui appartient à la portée *Applis* ne recevra que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis qui correspondent à la charge de travail
2. Politiques par défaut Applis
3. Politique collectrice Applis

Une charge de travail qui appartient aux portées *Applis* et *Applis Commerce* ne reçoit que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis
2. Politiques absolues Applis Commerce
3. Politiques par défaut Applis Commerce
4. Politiques par défaut Applis
5. Politique collectrice Applis Commerce

Une charge de travail qui appartient aux portées *Applis* et *Applis RH* ne recevra que les politiques suivantes dans l'ordre donné :

1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques par défaut Applis RH
4. Politiques par défaut Applis
5. Politique collectrice Applis RH

Ordre des politiques et chevauchement des portées

Important Le scénario suivant comporte des portées qui se chevauchent. Vous devez éviter que des portées connexes ne se chevauchent : les charges de travail ne doivent pas être membres de plusieurs branches de l'arborescence de la portée. Pour en savoir plus, consultez Chevauchement de portée, on page 370.

Une charge de travail qui appartient aux trois portées *Applis*, *Applis RH* et *Applis Commerce* recevra les politiques suivantes dans l'ordre donné :

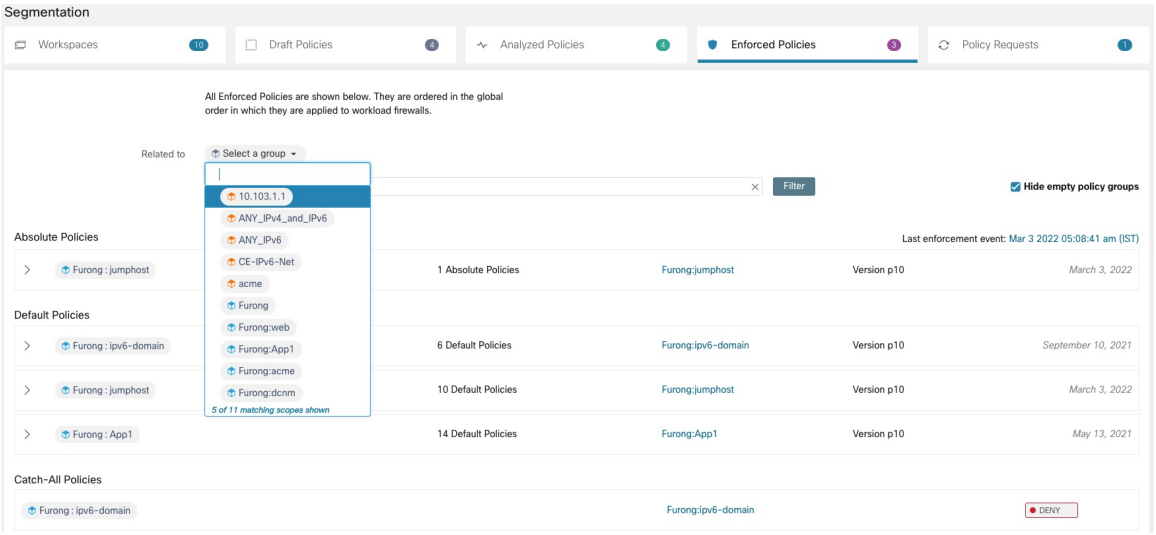
1. Politiques absolues Applis
2. Politiques absolues Applis RH
3. Politiques absolues Applis Commerce
4. Politiques par défaut Applis Commerce
5. Politiques par défaut Applis RH
6. Politiques par défaut Applis
7. Politique collectrice Applis Commerce

Notez que l'ordre relatif des portées *Applis RH* et *Applis Commerce* n'a d'importance que si les deux portées se chevauchent (c'est-à-dire si certaines charges de travail appartiennent aux deux portées connexes). En effet, les politiques sont toujours définies dans une portée. Une charge de travail appartenant à une seule portée ne sera pas affectée par les politiques de l'autre portée, donc l'ordre n'a pas d'importance.

Valider l'ordre et la priorité des politiques

Pour valider l'ordre et la priorité des politiques dans les espaces de travail parents/ancêtres, cliquez sur l'onglet **Analyzed Policies** (Politiques analysées) ou **Enforced Policies** (Politiques appliquées) en haut de la page Defend (Défendre) > Segmentation (Segmentation). Ces affichages fournissent une vue globale des politiques analysées et appliquées respectivement.

Figure 282: Exemple : liste des politiques appliquées par ordre de priorité



- Pour limiter la liste de politiques à celles qui incluent une portée ou un filtre particulier en tant que consommateur ou fournisseur, sélectionnez une portée ou saisissez un filtre.
- Filtres disponibles :

Nom du filtre	Définition
Port	Port de politique à mettre en correspondance, par exemple 80.
Protocol	Protocole de politique à mettre en correspondance, p. ex., TCP.
Approuvé	Correspond aux politiques qui ont été marquées comme Politiques approuvées
External? (Externe?)	Politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes.
Action	Action de la politique : Allow (Autoriser) ou Deny (Refuser)

(Avancé) Modifier les priorités de la politique

⚠

Mise en garde Il est rarement nécessaire de modifier l'ordre de priorité des politiques de portée. Étant donné que la modification des priorités des politiques peut affecter les résultats de la mise en application sur tous les espaces de travail, procédez avec prudence.

L’accès à cette fonctionnalité est limité aux utilisateurs ayant des rôles à privilèges très élevés, tels qu’un administrateur du site.

Avant de commencer

Avant de modifier l’ordre de priorité de la portée :

- Comprendre la logique de tri des politiques et comment les priorités des politiques sur les portées se reflètent dans l'ordre des intents de politique individuelles. Consultez Priorités des politiques, à la page 516.
- Effectuez les modifications dans un espace de travail secondaire jusqu'à ce que vous soyez sûr que le nouvel ordre sera conforme aux attentes.
- Planifiez vos modifications en tenant compte des directives suivantes :

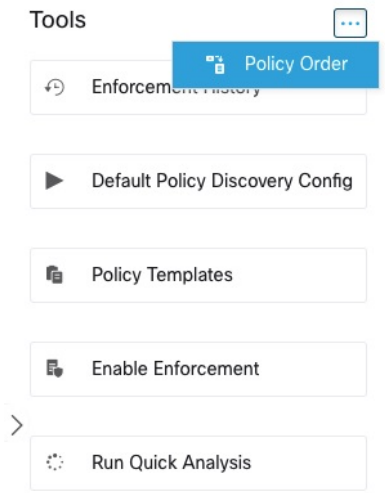
  Lors de la réorganisation, conservez l'ordre des parents en premier (les portées parents au-dessus des portées enfants) afin de tirer parti de la structure hiérarchique de votre arborescence de portées.

  (Si vous avez des portées jumelles qui se chevauchent, il peut être nécessaire de réorganiser ces dernières et leurs enfants. Le chevauchement des portées n'est pas recommandé. Corrigez ces problèmes en mettant à jour les requêtes de portée. Voir Chevauchement de portée, à la page 370).

Procédure

Étape 1 Pour réorganiser la priorité des politiques, cliquez sur l'icône de menu à côté de **Tools** (Outils) et sélectionnez **Policies Order** (Ordre des politiques) :

Illustration 283 : Accès à la page des priorités de politique

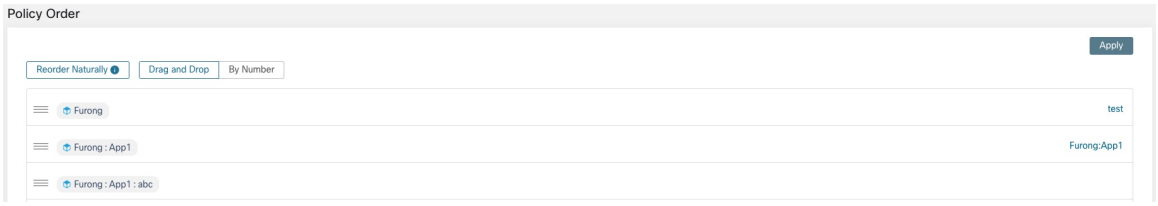


Une fois sur la page de l'ordre des politiques, vous pouvez voir la liste de toutes les portées et de leurs espaces de travail principaux correspondants en fonction de la priorité actuelle des politiques.

Étape 2 Il existe plusieurs façons de réorganiser les portées :

- Pour réorganiser la liste complète afin de placer les portées parentes au-dessus des portées enfants (« ordre préalable ») : Cliquez sur **Réorganiser naturellement**. Il s'agit de l'ordre recommandé et tout écart par rapport à cet ordre doit être effectué avec prudence.
- Pour réorganiser la liste manuellement :
  - Faites glisser les lignes vers le haut ou vers le bas.
  - Cliquez sur **By Number** (By numéro) pour définir un numéro pour chaque portée à utiliser pour le tri. Cela peut être plus facile pour les listes volumineuses.

Illustration 284 : Définition des priorités de politique pour les portées



Prochaine étape

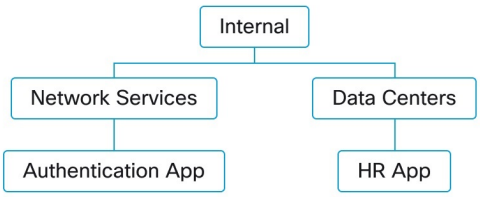
Exécutez l'analyse rapide pour afficher les résultats de vos modifications.

Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques

Exemple de scénario

La situation suivante est un exemple illustrant le trafic entre portées :

Votre hiérarchie de portée comprend une portée de services réseau qui comprend une application d'authentification (le fournisseur). Une application RH, membre d'une portée située sur une autre branche de la hiérarchie des portées, est un consommateur du service fourni par l'application d'authentification.



Options de politiques

Cisco Secure Workload offre plusieurs façons de résoudre cette situation :

Option	Instructions	Avantages et inconvénients
Créez ces politiques dans une portée parente ou ancestrale qui inclut à la fois le consommateur et le fournisseur en tant qu'enfants ou descendants.	• Créez manuellement une ou plusieurs politiques dans la portée ancestrale commun. (Facultatif) Pour des politiques plus précises, regroupez les charges de travail à l'aide de filtres d'inventaire. Pour obtenir des exemples et des instructions, consultez Créer un filtre d'inventaire, on page 392. • Détectez automatiquement les politiques dans la portée ancestrale commune, pour la branche entière de l'arborescence de la portée.	Ces méthodes constituent le moyen le plus simple d'aborder les politiques à portée multiple. Ces méthodes ne nécessitent qu'une seule politique par paire consommateur-fournisseur. Si vous envisagez d'utiliser la découverte automatique des politiques, consultez les considérations importantes dans Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, on page 453.
Utiliser la méthode avancée pour créer des politiques à portées croisées	Détectez automatiquement les politiques pour chaque portée. Consultez (Avancé) Créer des politiques de portées croisées, on page 523. (Cette procédure s'applique aux politiques créées manuellement et aux politiques découvertes).	Cette méthode nécessite deux politiques pour chaque paire client-fournisseur : une politique pour le client et une pour le fournisseur. Cette méthode permet la création de politiques lorsque les politiques d consommateur et du fournisseur appartiennent à des personnes différentes. reportez-vous aux autres considérations en Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, on page 453.

(Avancé) Créer des politiques de portées croisées

Cette procédure décrit la méthode avancée de création de politiques à portée croisée (politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes). Elle s'applique aux politiques créées manuellement et aux politiques détectées automatiquement.

Cette méthode nécessite deux politiques pour chaque paire consommateur-fournisseur, car les deux extrémités de la conversation doivent autoriser la conversation :

- Une politique dans la portée consommateur doit autoriser les conversations avec le fournisseur,

  et

- Une politique dans la portée du fournisseur doit autoriser les conversations avec le consommateur.

Cette procédure comprend les étapes qui doivent être suivies par le propriétaire de chaque portée afin de créer des politiques inter-portées. Si vos privilèges d'accès vous permettent de modifier les deux portées, vous pouvez effectuer toutes les étapes.

Avant de commencer

- Envisagez des options plus simples pour gérer le trafic entre les portées. Consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, à la page 522.
- Les politiques qui utilisent cette méthode doivent être créées dans l'espace de travail principal du consommateur et du fournisseur.

  Si la portée du fournisseur à spécifier dans la politique n'a pas encore d'espace de travail principal, créez-le avant de créer des politiques de portée croisée à l'aide de cette méthode.
- Les politiques doivent comporter l'action ALLOW (AUTORISER) pour que des demandes de politiques soient créées.
- Pour plus de détails sur ces exigences, consultez Demandes de politiques, à la page 525.
- (Facultatif) Envisagez des options de traitement automatique des demandes de politiques à portée croisée. Consultez Automatiser le traitement des demandes de politique globales, à la page 529.
- (Facultatif) Si vous souhaitez que les politiques multiportées ne s'appliquent qu'aux charges de travail d'une grappe dans la portée du consommateur ou du fournisseur, et non à la portée entière, consultez Convertir une grappe en filtre d'inventaire, à la page 510. Les grappes ne peuvent pas être utilisées dans les politiques à portée croisée créées à l'aide de cette procédure.

  Si vous détectez les politiques automatiquement, consultez aussi Dépendances externes, à la page 462 et Ajuster les dépendances externes d'un espace de travail, à la page 464.

Procédure

Étape 1 Dans l'espace de travail principal du consommateur, créez la politique souhaitée, manuellement ou à l'aide de la découverte automatique des politiques.

Pour chaque politique inter-portée créée, une demande de politique est automatiquement créée pour le fournisseur.

Pour afficher les demandes de politique, consultez Affichage, acceptation et refus des demandes de politique, à la page 525.

Remarque : Si une politique existante dans l'espace de travail de l'application du fournisseur correspond à ce trafic, une nouvelle politique n'est pas nécessaire et la demande n'est pas créée. Cette situation est signalée comme décrit dans Demandes de politiques résolues, à la page 533.

Étape 2 Vous (ou le propriétaire de l'application du fournisseur) devez répondre à chaque demande de politique :

Consultez Affichage, acceptation et refus des demandes de politique, à la page 525.

L'acceptation d'une demande de politique crée automatiquement la politique requise dans l'espace de travail principal du fournisseur, permettant le trafic entre les deux applications.

Si vous ne souhaitez pas autoriser le trafic de l'application requérante, rejetez la demande.

Étape 3 (Facultatif) Si vous découvrez automatiquement les politiques, vous pouvez Ajuster les dépendances externes d'un espace de travail, à la page 464.

Étape 4 Passez en revue et analysez les deux espaces de travail principaux.

Prochaine étape

Lorsque vous êtes prêt à appliquer ces politiques, vous devez les appliquer sur les deux espaces de travail principal.

Demandes de politiques

Les demandes de politique sont générées lorsque vous créez des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 523. Chaque fois qu'une politique est créée dans l'espace de travail principal d'une portée de consommateur lorsque le fournisseur est membre d'une portée différente, si la politique n'existe pas encore dans l'espace de travail principal associé à la portée du fournisseur, une demande de politique est générée.

Cette demande de politique alerte le propriétaire de l'application du fournisseur pour permettre aux applications tributaires d'accéder aux services nécessaires.

Consultez les options d'affichage et de réponse aux demandes de politique aux adresses Affichage, acceptation et refus des demandes de politique, on page 525 et Automatiser le traitement des demandes de politique globales, on page 529.

Renseignements supplémentaires sur les demandes de politique

- La page des services fournis (sur laquelle les demandes de politique apparaissent) n'est disponible que pour les espaces de travail principaux. Ainsi, des expériences isolées sur des espaces de travail secondaires ne créent pas de notifications dans d'autres espaces de travail principaux.
- Si une portée externe (lorsque le fournisseur spécifié dans la politique appartient à une autre portée que le consommateur) n'a pas d'espace de travail principal, aucune demande n'est envoyée (par exemple, cela peut être le cas pour la portée racine ou toute autre portée définie pour les charges de travail à l'extérieur de l'organisation). Si une portée externe n'a publié aucune politique, l'analyse et l'application de la politique sont effectuées du côté consommateur uniquement.
- Les grappes ne sont pas prises en charge lorsque le fournisseur se trouve dans une portée différente de celle du consommateur. Si le consommateur de la politique est une grappe, la demande de politique sera effectuée comme si la demande de politique provenait de la portée de l'application consommateur. Plusieurs politiques utilisant le même service d'un fournisseur pourraient être regroupées.
- Les demandes de politiques sont générées uniquement pour les fournisseurs, et non pour les consommateurs. Si un espace de travail consommateur analyse ou applique des politiques, il doit inclure explicitement des politiques qui autorisent tous ses flux de consommation légitimes, soit par le biais de la découverte automatique des politiques, soit en élaborant explicitement des politiques (aucune demande de politiques des espaces de travail de fournisseurs externes n'est générée).

Affichage, acceptation et refus des demandes de politique

Lors de la création de politiques multiportées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 523, une politique est requise dans l'espace de travail principal de la portée du fournisseur en plus de la politique dans la portée du consommateur. Lorsqu'une politique multiportée est créée dans l'espace de travail principal de la portée du consommateur, une demande de politique est automatiquement créée dans l'espace de travail principal de la portée du fournisseur.

Utilisez les informations de cette rubrique pour accepter la demande (pour créer la politique requise dans la portée du fournisseur) ou rejeter la demande (auquel cas la politique multiportée ne prendra pas effet).

Pour afficher, accepter ou refuser des demandes de politique :

Destinataire	Faire ceci
Afficher toutes les demandes de politique	**1.** Choisissez **Defend (défense) > Segmentation (segmentation).** **2.** Cliquez sur **Policy Requests** (Demandes de politiques) en haut de la page. **3.** Cliquez sur une portée de consommateur pour afficher les demandes de politique de cette portée.
Afficher les demandes de politique pour une portée particulière	Pour afficher les demandes de politique en attente pour la portée d'un fournisseur : **1.** Choisissez **Defend (défense) > Segmentation (segmentation).** **2.** Cliquez sur l'espace de travail principal de la portée applicable. **3.** Cliquez sur **Manage Policies** (Gestion des politiques). **4.** Cliquez sur **Provided Services** (Services fournis). Si l'onglet n'affiche pas un numéro, il n'y a aucune demande de politique en attente pour cet espace de travail. **5.** Cliquez sur **Policy Requests**(demandes de politiques). **6.** Cliquez sur une portée de consommateur pour afficher les demandes de politique de cette portée. Ou Pour afficher une demande de politique à partir de la portée consommateur : Dans l'onglet Policies (Polices) de l'espace de travail principal de la portée consommateur, cliquez sur la valeur de la colonne **Protocols and Ports** (protocoles et ports), puis examinez le panneau qui s'ouvre sur le côté droit de la page. Dans la section **Protocols and Ports** (protocoles et ports), cliquez sur un point jaune pour voir les demandes de politique en attente.
Accepter manuellement une demande et créer automatiquement la politique requise dans la portée du fournisseur	À partir de l'un des emplacements ci-dessus, cliquez sur **Accept** (accepter) à côté de la demande de politique.
Rejeter manuellement une demande	À partir de l'un des emplacements ci-dessus, cliquez sur **Reject** (Rejeter) à côté de la demande de politique.

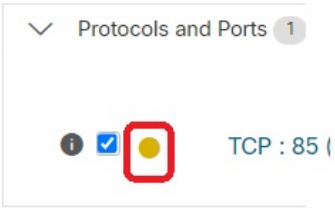
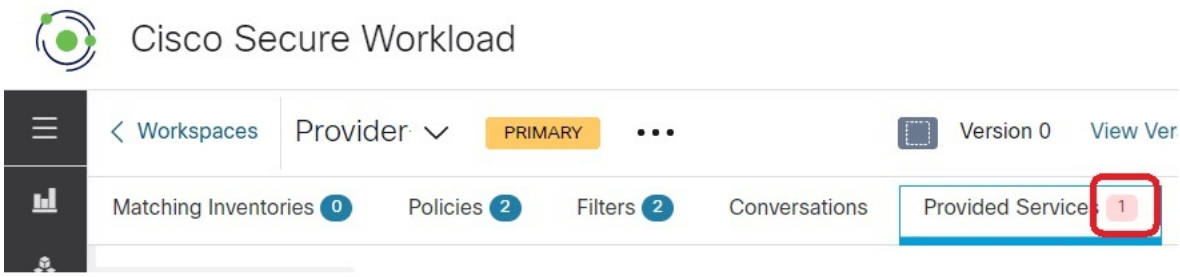
Destinataire	Faire ceci
Afficher l'état de la demande de politique à partir de l'espace de travail du consommateur	Dans la page Policies (Politiques) de l'espace de travail du consommateur principal, cliquez sur la politique, puis sur la valeur du port/du protocole. L'état est affiché dans le panneau qui s'ouvre sur la droite. Les demandes en attente sont accompagnées d'un point jaune :  Lorsque la demande est acceptée, le point se transforme en coche verte :  Cliquez sur l'indicateur pour en savoir plus.
Afficher l'état de la demande de politique à partir de l'espace de travail du fournisseur	Afficher l'état de la demande sous l'onglet **Provided Services** (Services fournis) décrit ci-dessus.
Autoriser la découverte de politiques à créer la politique requise pour le fournisseur	Détectez automatiquement les politiques dans l'espace de travail principal de la portée du fournisseur en utilisant une plage temporelle qui garantit que les flux correspondants sont visibles, puis publiez la politique.
Consultez aussi les options d'automatisation du traitement des demandes de politique	Automatiser le traitement des demandes de politique globales, on page 529

Figure 285: Demandes de politique en attente dans l'espace de travail du fournisseur



Acceptation des demandes de politique : détails

Accepter une demande de politique sur un service équivaut à créer une politique à partir du filtre demandé, en tant que consommateur, vers le service, en tant que fournisseur. De plus, lors de l'acceptation d'une demande de politique, la politique d'origine de l'espace de travail de l'application consommateur (dans l'exemple, l'application frontale et la couche de service) sera marquée comme acceptée (voir les figures i-dessous).

Figure 286: Acceptation/rejet des demandes de politique

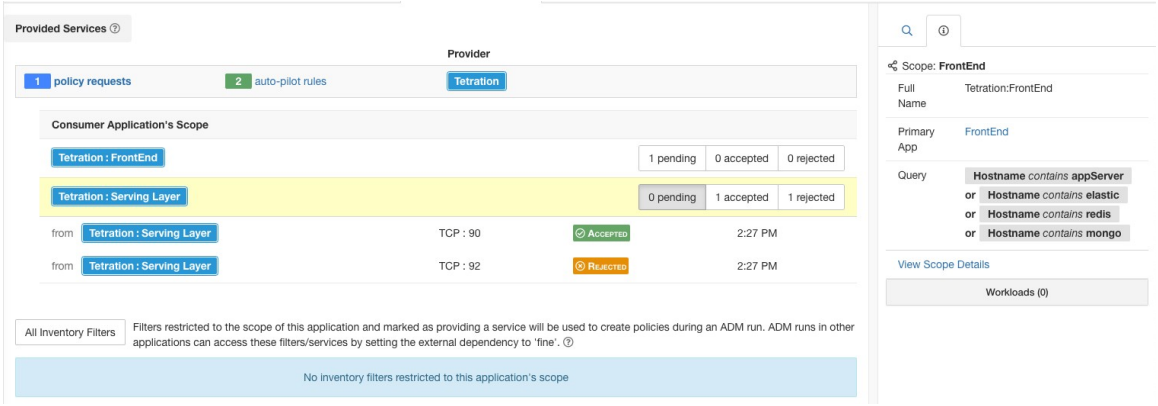
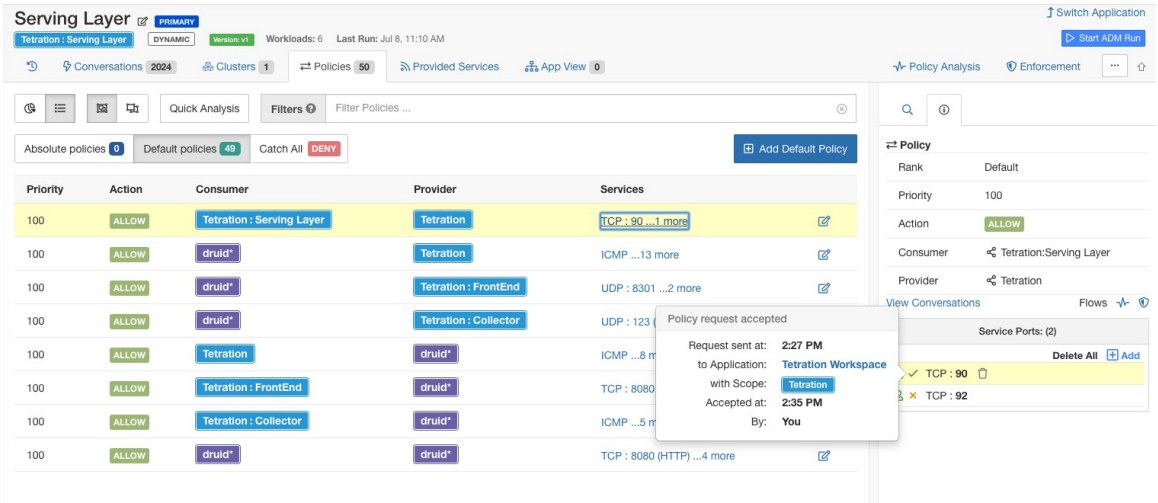


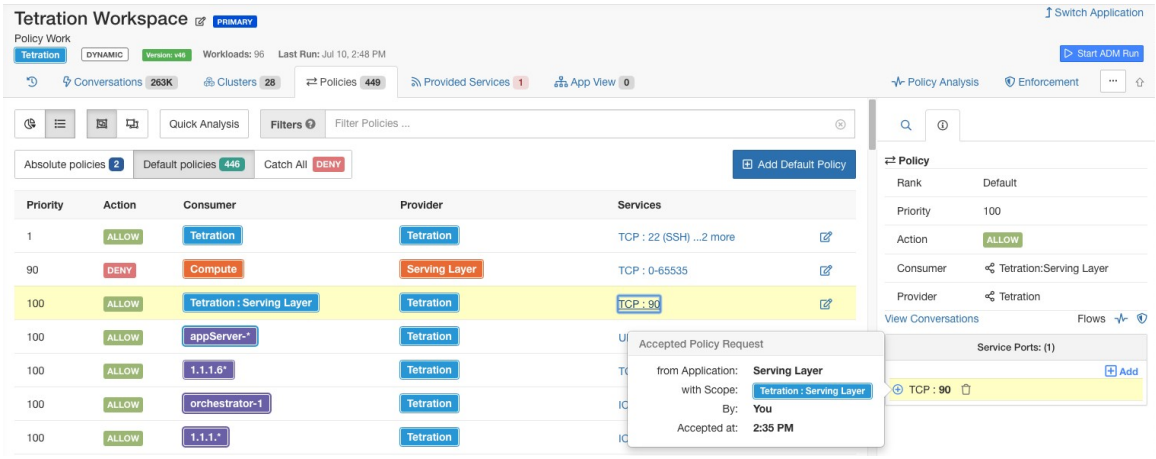
Figure 287: État de la politique affiché comme accepté



La nouvelle politique créée sur l'espace de travail de l'application du fournisseur (dans cet exemple, l'espace de travail est nommé Tetration) est marquée d'un icône **plus** indiquant que cette politique a été créée en raison d'une demande de politique externe.

Note Si la politique d'origine du côté du consommateur est supprimée après l'acceptation de la demande de politique, la politique du côté du fournisseur ne sera pas supprimée. Cependant, l'info-bulle à côté de la politique indique que la politique d'origine a été supprimée avec l'horodatage de l'événement :

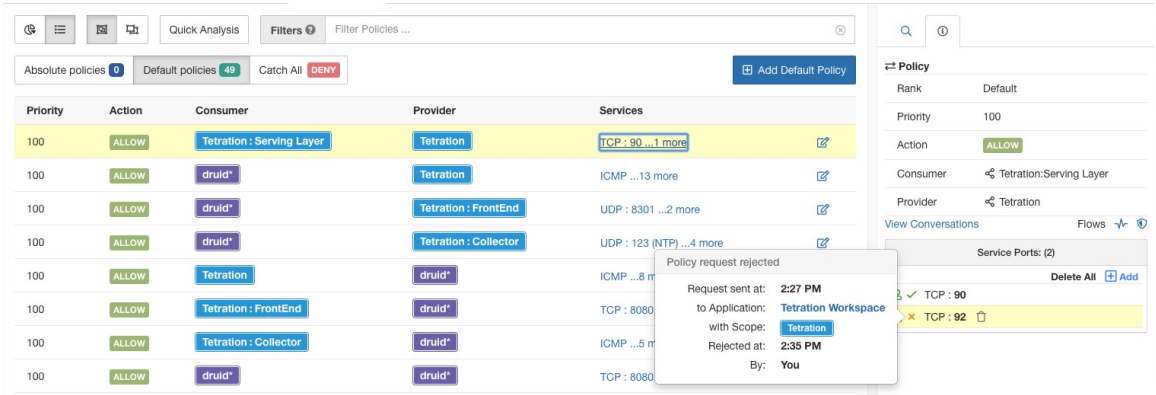
Figure 288: Politique du côté du fournisseur, créée en acceptant une demande de politique



Rejet des demandes de politique : Détails

Le rejet d'une demande de politique n'entraîne ni la création ni la mise à jour de politiques. La politique d'origine de l'espace de travail de l'application consommateur (dans l'exemple, application de la couche de service) sera marquée comme rejetée, mais la politique reste en vigueur, c'est-à-dire que le trafic sortant sera toujours autorisé. L'info-bulle à côté de la politique de rejet contient des informations sur l'application du fournisseur, l'utilisateur qui a rejeté la demande de politique ainsi que l'heure du rejet.

Figure 289: État de la politique affiché comme Rejeté



Automatiser le traitement des demandes de politique globales

Les demandes de politique sont générées lorsque vous créez des politiques inter-portées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, à la page 523.

Il existe plusieurs options pour réduire le nombre de demandes de politiques générées lors de la création de politiques inter-portées :

Tableau 27 : Options de traitement automatique des demandes de politique

Destinataire	Faire ceci
Préciser le traitement des demandes de politique entre des paires consommateur-fournisseur données	Consultez Règles de pilote automatique, à la page 530. Vous devez avoir les privilèges requis.
Créer automatiquement toutes les politiques requises pour les fournisseurs pour toutes les politiques de portées croisées créées lors de la découverte de politiques dans un espace de travail en particulier	Lorsque vous démarrez une exécution de découverte automatique de politique, activez l'option d' **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politique sortants) dans la section Advanced Configurations (Configurations avancées). Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site. Pour de plus amples renseignements, consultez la section : Configurations avancées pour la découverte automatique des politiques, à la page 467 et Connecteurs de politiques d'acceptation automatique, à la page 532
Préciser le traitement par défaut pour toutes les demandes de politique de tous les espaces de travail	Dans la page de configuration de la découverte des politiques par défaut, activez l'option **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politiques sortants) dans la section Advanced Configurations (configurations avancées). Cette option est disponible uniquement pour les propriétaires de portée racine et les administrateurs de site. Pour de plus amples renseignements, consultez la section : Configuration de la découverte de politiques par défaut, à la page 477 et Configurations avancées pour la découverte automatique des politiques, à la page 467 et Connecteurs de politiques d'acceptation automatique, à la page 532

Règles de pilote automatique

Cette fonctionnalité est applicable uniquement si vous créez des politiques à portée croisée en utilisant la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 523.

Les applications d'infrastructure qui fournissent des services à de nombreuses autres applications dans un centre de données peuvent recevoir un grand nombre de demandes de politique d'autres applications.

Vous pouvez réduire le volume des demandes de politiques en créant des règles de pilote automatique pour accepter ou rejeter automatiquement les futures demandes de politiques correspondantes.

Note Les règles du pilote automatique ne s'appliquent pas aux demandes de politiques existantes. Elles affectent uniquement les demandes de politiques futures.

Accepter ou rejeter automatiquement les demandes de politique à l'aide des règles de pilote automatique

Configurez les règles de pilote automatique pour accepter ou rejeter automatiquement les demandes de politique entre une paire consommateur-fournisseur donnée, sur des ports précisés. Les règles du pilote automatique peuvent être larges (portée à portée) ou s'appliquer uniquement à un sous-ensemble de charges de travail dans chaque portée (comme configuré par les filtres d'inventaire. Vous pouvez utiliser un filtre d'inventaire pour le consommateur, pour le fournisseur ou pour chacun d'entre eux).

1. Si vous souhaitez que votre règle de pilote automatique s'applique à un sous-ensemble de charges de travail au sein d'une portée plutôt qu'à l'ensemble de la portée :

   Créez un filtre d'inventaire dans la ou les portées pertinentes pour regrouper les charges de travail. Assurez-vous que l'option **Restrict Query to Ownership Scope** (Restreindre la requête à la portée de propriété) est sélectionnée dans chaque filtre d'inventaire, pour vous assurer que le filtre n'inclut que les charges de travail qui sont membres de la portée.

2. Choisissez **Defend (défense) > Segmentation (segmentation).**

3. Cliquez sur l'espace de travail principal de la portée du consommateur pour laquelle vous souhaitez accepter ou rejeter automatiquement les demandes de politique liées à un fournisseur spécifique.

4. Cliquez sur **Manage Policies** (Gestion des politiques).

5. Cliquez sur **Provided Services** (Services fournis).

6. Si vous créez cette règle pour un filtre d'inventaire, effectuez les étapes suivantes pour le filtre d'inventaire souhaité (les filtres d'inventaire sont identifiés par une icône orange).

   Sinon, effectuez ces étapes pour la portée (les portées sont identifiées par une icône bleue).

   Assurez-vous de cliquer au bon endroit.

7. Cliquez sur **No Auto-Pilote Rules** (aucune règle de pilote automatique) ou sur **auto-pilot Rules** (règles de pilote automatique), selon ce qui est affiché.

8. Cliquez sur **New Auto-Pilote Rule** (nouvelle règle de pilote automatique).

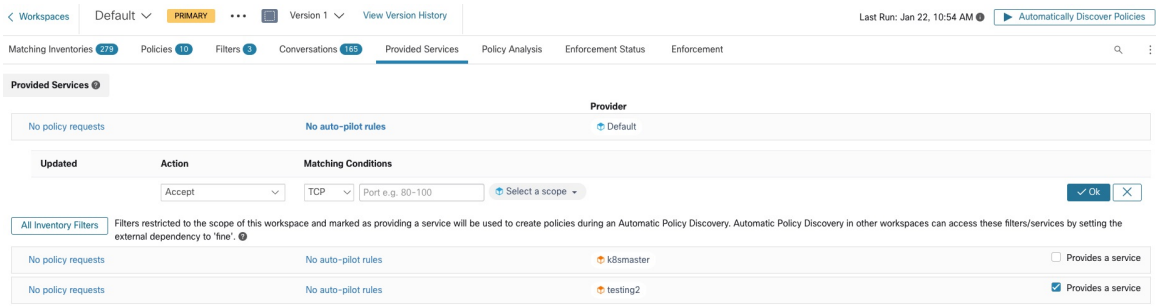
9. Configurez la règle de pilote automatique. Sélectionnez la portée ou le filtre d'inventaire qui représente le fournisseur.

10. Cliquez sur **OK**.

Exemple de règle de pilote automatique

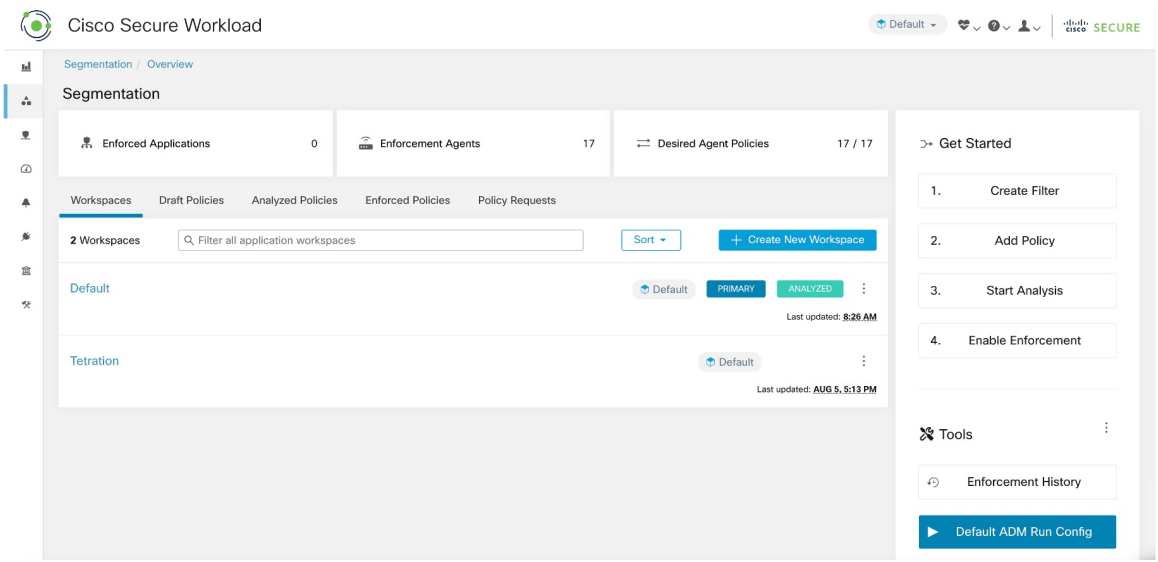
Dans l'exemple ci-dessous, nous créons une nouvelle règle de pilote automatique pour rejeter les demandes de politique TCP dans la plage de ports 1 à 200 de tout consommateur contenu dans Tetration:Adhoc du service du fournisseur Tetration

Figure 290: Création/mise à jour des règles du pilote automatique



Ensuite, nous créons une nouvelle politique dans l'espace de travail pour l'*application frontale* sur le port TCP 23. Comme la politique correspond à la règle de pilote automatique, elle sera automatiquement rejetée. L'état et le motif du refus de la politique sont indiqués dans l'info- bulle à côté de la politique rejetée.

Figure 291: Politique automatiquement rejetée par la règle de pilote automatique



Afficher le nombre des politiques récemment créées par les règles de pilote automatique

Pour afficher le nombre de politiques créées dans un espace de travail par les règles de pilote automatique depuis le dernier lancement (ou redémarrage) de l'analyse des politiques pour l'espace de travail :

Accédez à la page des services fournis pour l'espace de travail principal concerné et recherchez le nombre de politiques « créées automatiquement ».

Connecteurs de politiques d'acceptation automatique

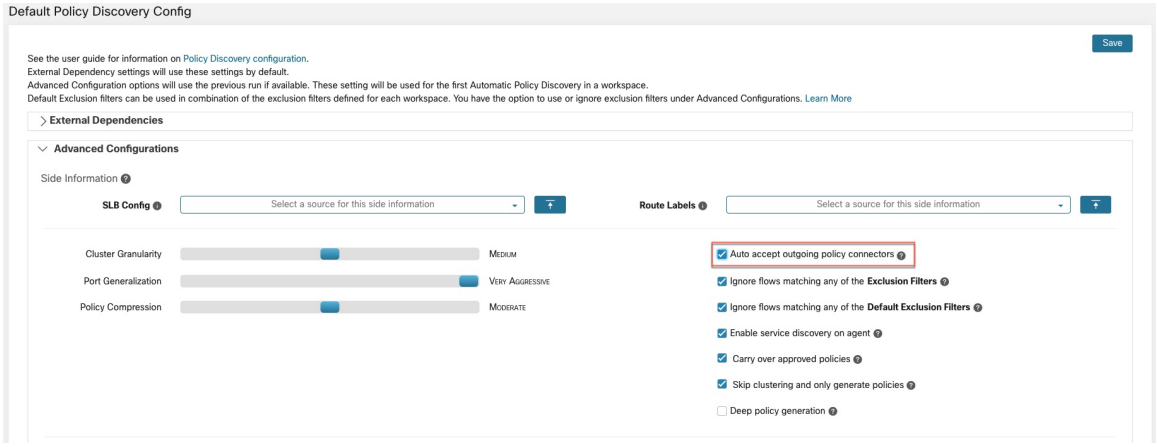
Vous pouvez définir cette option comme configuration de découverte de politiques par défaut, ou la définir dans les options avancées de découverte automatique des politiques pour chaque espace de travail.

L'option **Auto accept outgoing policy connectors** (Acceptation automatique des connecteurs de politique sortants) de la page de configuration de la découverte automatique des politiques vous permet d'accepter automatiquement toutes les demandes de politique créées dans le cadre de la découverte automatique des politiques.

Si cette option est activée dans la configuration de découverte automatique des politiques par défaut, les demandes de politiques créées manuellement ou en important un espace de travail seront également automatiquement acceptées.

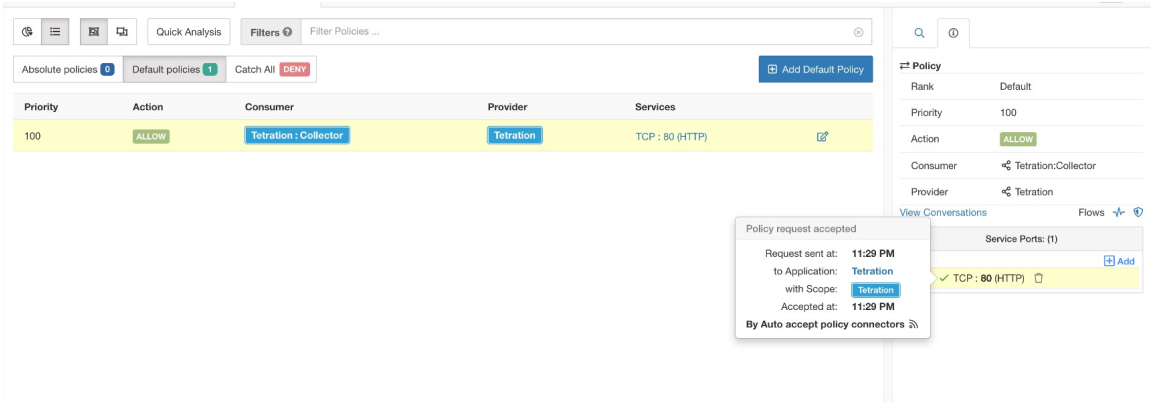
Note Cette option est uniquement disponible pour les propriétaires de portée racine ou les administrateurs de site .

Figure 292: L'option d'acceptation automatique des connecteurs de politique sortants



Une fois cette option définie, toute demande de politique créée dans un espace de travail, la portée racine ou dans l'espace de travail concerné sera automatiquement acceptée.

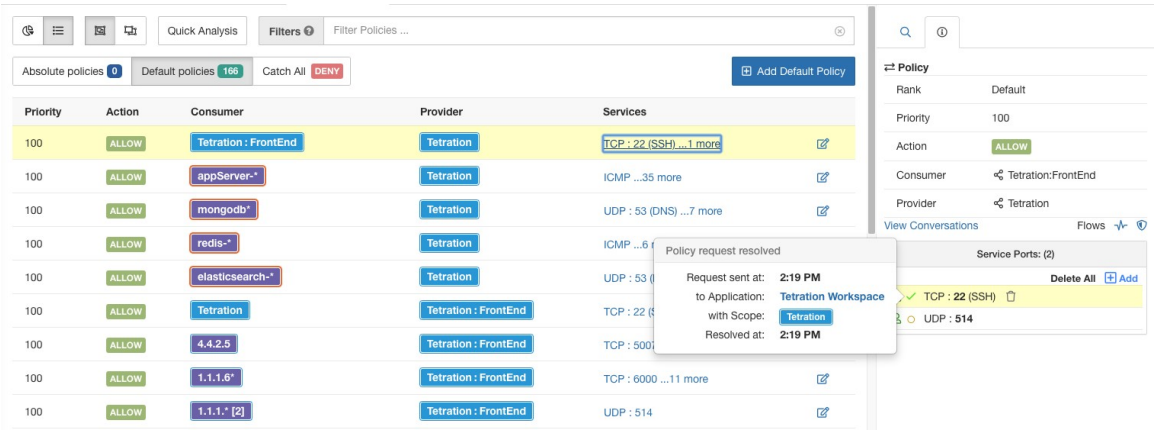
Figure 293: La politique est automatiquement acceptée par les connecteurs d'acceptation automatique de politiques



Demandes de politiques résolues

Si toutes les conditions pour la création d'une demande de politique sont réunies, mais qu'il existe déjà une politique correspondante sur l'espace de travail du fournisseur, la politique créée sur l'espace de travail de l'application client sera marquée comme résolue, ce qui indique que l'espace de travail de l'application du fournisseur autorise déjà le trafic. le port demandé.

Figure 294: État de la politique affiché comme Résolu



Services fournis

Cette page est utilisée uniquement pour la création de politiques dans lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes, et uniquement si vous utilisez la méthode décrite dans (Avancé) Créer des politiques de portées croisées, on page 523.

Pour plus d'informations sur cette option, consultez :

- Demandes de politiques, on page 525
- Règles de pilote automatique, on page 530
- Créer un filtre d'inventaire, on page 392 et Dépendances externes, on page 462 (pour en savoir plus sur l'option **fournit un service**)

Pour accéder à cette page, accédez à un espace de travail principal, cliquez sur **Manage Policies** (Gérer des politiques), puis sur **Provided Services** (Services fournis).

Dépannage des politiques de portées croisées

Si des politiques de portée croisée ont été créées à l'aide de la méthode décrite dans (Avancé) Créer des politiques de portées croisées, à la page 523, les espaces de travail principaux pour les charges de travail des consommateurs et des fournisseurs doivent chacun avoir une politique qui autorise le trafic. Assurez-vous que les politiques requises existent dans les deux espaces de travail.

Aucune notification n'est envoyée si l'une des politiques est supprimée ou modifiée.

Si la paire de politiques a été générée lors de la recherche de celles-ci, consultez les informations relatives à l'approbation des politiques afin de les protéger contre les recherches ultérieures. Consultez Approuver les politiques, à la page 479.

Vérifiez que les autres exigences sont toujours respectées, comme indiqué dans (Avancé) Créer des politiques de portées croisées, à la page 523.

Des espaces de travail pour les consommateurs et les fournisseurs ayant les politiques requises doivent être mis en application.

Outils utiles pour les politiques multi-portées

- Utiliser le filtre **External?** (Externe?) pour trouver les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle dans laquelle vous avez découvert les politiques.
- La vue des politiques comporte une option permettant d'afficher les politiques externes. Consultez Représentation visuelle des politiques, à la page 542.

Si vous utilisez la configuration de découverte de politiques par défaut

Assurez-vous d'avoir cliqué sur **Save** (enregistrer) dans la page **Default Policy Discovery Config** (configuration de la découverte des politiques par défaut) après avoir apporté des modifications pour rendre les configurations de dépendances externes par défaut disponibles pour les espaces de travail individuels.

Consommateur ou fournisseur réel

Le consommateur et le fournisseur spécifiés dans une politique déterminent :

- L'ensemble des charges de travail dotées de d'agents Cisco Secure Workloadqui reçoivent la politique.
- L'ensemble des adresses IP qui sont affectées par les règles de pare-feu installées.

Par défaut, ce sont les mêmes.

Cependant, vous devrez peut-être spécifier un groupe d'adresses IP dans les règles de pare-feu différent des adresses IP des charges de travail qui reçoivent la politique. (Voir un exemple ci-dessous).

Pour répondre à ce besoin, vous pouvez configurer le consommateur et le fournisseur effectifs.

Comportement par défaut pour le consommateur et le fournisseur

Par défaut, lorsqu'un agent Cisco Secure Workload reçoit une politique, les règles de pare-feu sont spécifiques à cette charge de travail. C'est ce que l'exemple suivant illustre le mieux :

Considérons une politique ALLOW avec un filtre de fournisseur spécifiant le sous-réseau 1.1.1.0/24. Lorsque cette politique est programmée sur un charge de travail avec l'adresse IP 1.1.1.2, les règles de pare-feu se présentent comme suit :

- Pour le trafic entrant, les règles de pare-feu autorisent le trafic destiné à la version 1.1.1.2 en particulier et non à l'ensemble du sous-réseau 1.1.1.0/24.
- Pour le trafic sortant, les règles de pare-feu autorisent le trafic provenant dans la version 1.1.1.2 en particulier, et non de l'ensemble du sous-réseau 1.1.1.0/24 (pour éviter l'usurpation d'identité).

En corollaire, les charges de travail d'agent appartenant à l'espace de travail qui n'ont pas d'adresse IP dans le sous-réseau 1.1.1.0/24 ne recevront pas les règles de pare-feu ci-dessus.

Exemple : consommateur réel ou fournisseur réel

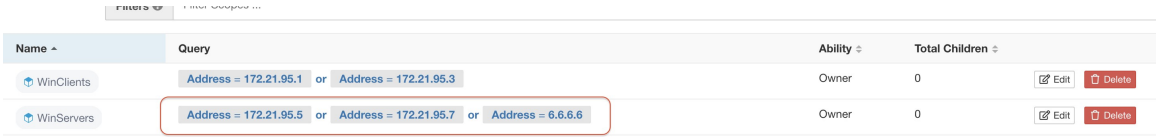
Dans cet exemple, supposons que vous configurez des politiques pour un parc de charges de travail derrière une adresse IP virtuelle (VIP), similaires aux solutions de mise en grappe Keepalive ou Windows avec basculement. Vous ferez appel à un consommateur ou à un fournisseur effectifs pour veiller à ce que le trafic ne soit pas interrompu lors d'un basculement.

Imaginez un parc de charges de travail avec des adresses IP (*172.21,95.5* et *172.21,95.7*) qui fournissent un service derrière une adresse VIP – *6.6.6.6*. Cette VIP est flottante et une seule charge de travail possède la

VIP à tout moment. L'objectif est de programmer des règles de pare-feu sur toutes les charges de travail du parc afin de permettre le trafic vers l'adresse *6.6.6.6*.

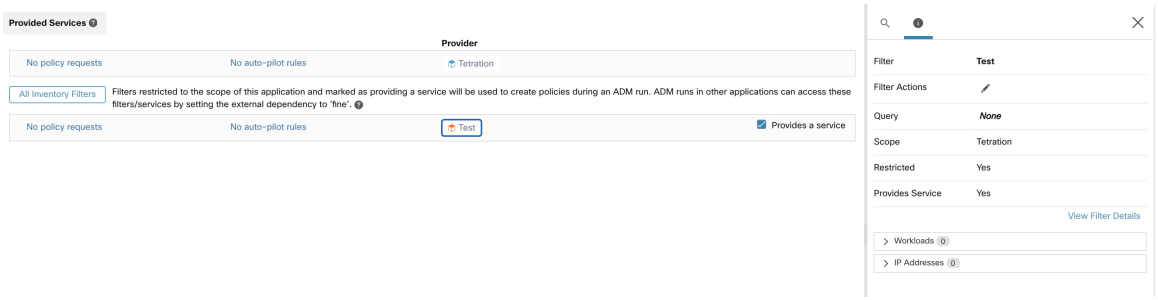
Dans cette configuration, nous avons un portée et un espace de travail correspondant qui contiennent un groupe de charges de travail qui représente le parc (*172.21,95.5* et *172.21,95.7*) ainsi que l'adresse VIP (*6.6.6.6*).

Figure 295: Portée incluant les VIP et les grappes de charges de travail



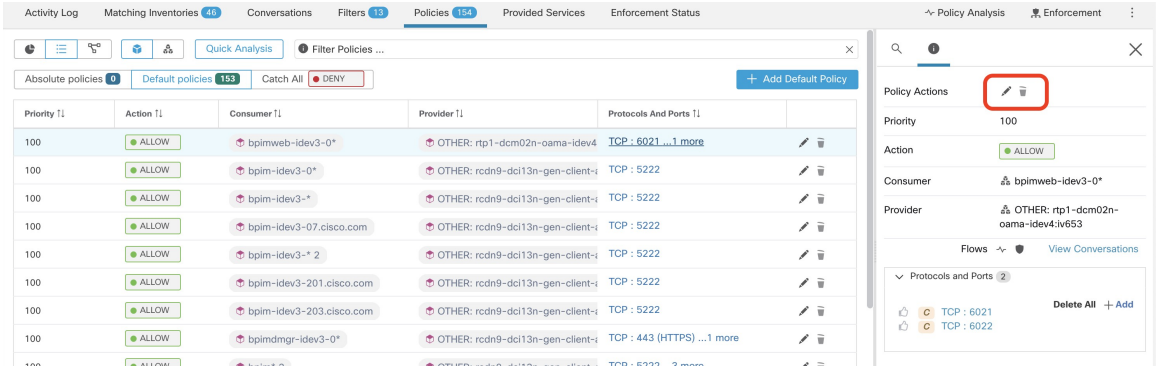
L'adresse VIP est accessible dans cet espace de travail en tant que service fourni, comme indiqué ci-dessous :

Figure 296: VIP accessible comme un service fourni



Si nous ajoutons une politique des clients de ce service à l'adresse VIP de service, les règles de pare-feu (par défaut) autorisant le trafic vers l'adresse VIP ne seront programmées que sur la charge de travail qui possède l'adresse VIP. Toutefois, en cas de basculement, il peut s'écouler un certain temps avant que la nouvelle charge de travail à laquelle appartient le service VIP ne reçoive les règles de pare-feu adéquates et le trafic peut être perturbé pendant un court laps de temps.

Figure 297: Politique autorisant le trafic des clients vers l'adresse VIP de service

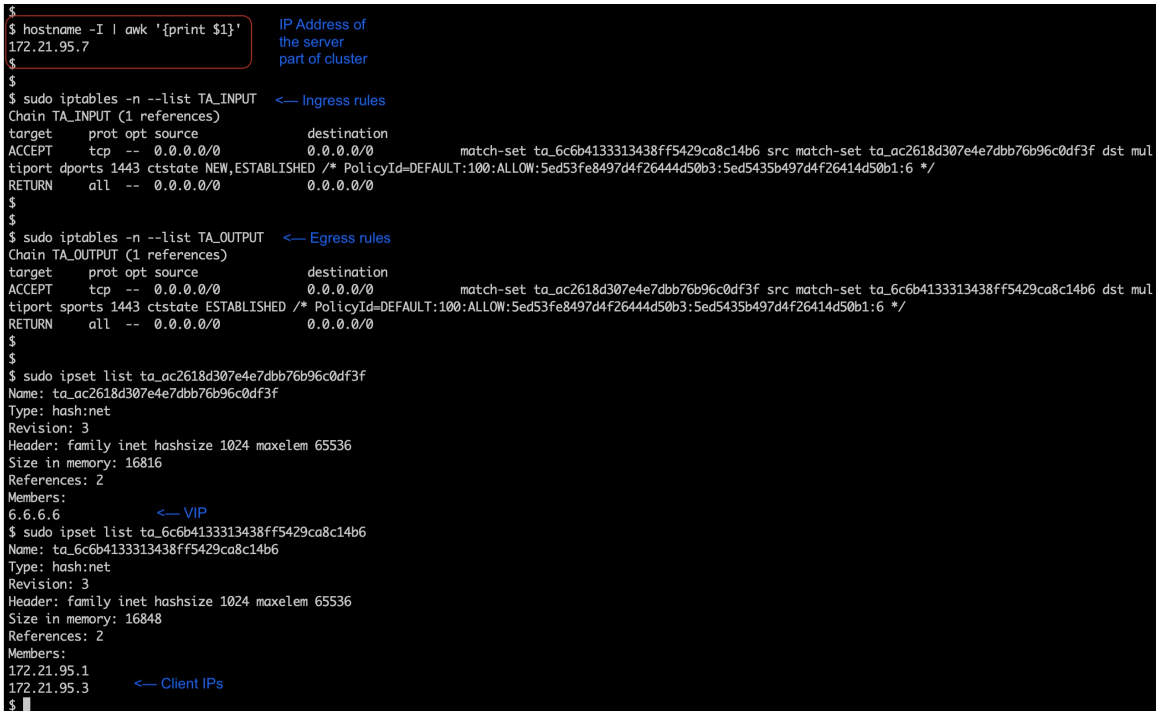


Pour résoudre ce problème, nous configurons le fournisseur effectif (en utilisant la procédure ci-dessous) Plus précisément, nous avons défini le fournisseur effectif de manière à inclure le groupe de charges de travail pour lesquelles des règles de pare-feu autorisant le trafic vers le service VIP doivent être programmées - peu importe que l'une de ces charges de travail possède ou non l'adresse VIP.

Lorsque le fournisseur effectif est défini, nous pouvons voir sur les charges de travail que les règles de pare-feu autorisant le trafic vers 6.6.6.6 sont programmées même lorsqu'une charge de travail ne possède pas l'adresse VIP. Lorsque toutes les charges de travail qui soutiennent le service sont programmées avec ces règles, le

trafic ne sera pas interrompu lors d'un événement de basculement, car les règles de pare-feu nécessaires seront programmées sur la nouvelle charge de travail principale (qui possède l'adresse VIP).

Figure 298: Règles de pare-feu sur l'hôte autorisant le trafic vers le service VIP



Comment configurer le consommateur réel ou le fournisseur réel

1. Cliquez sur la politique à modifier.
2. Cliquez sur le bouton Edit (modifier) dans le coin supérieur droit de la politique pour accéder aux options de politique avancées.
3. Cliquez sur **Effective Consumer** (Consommateur réel) ou **Effective Provider**(fournisseur réel).
4. Précisez les adresses souhaitées.
5. Vous devrez peut-être préciser des adresses à la fois pour le consommateur réel et pour le fournisseur réel.

À propos de la suppression de politiques

Important Avant de supprimer une politique, vérifiez qu'elle ne fait pas partie d'une paire de politiques requises lorsque le consommateur et le fournisseur se trouvent dans des portées différentes.

Pour le déterminer : Cliquez sur le lien de la politique dans la colonne Protocols and Ports (Protocoles et ports). Dans le panneau qui s'ouvre sur le côté droit de la page, examinez la section Protocols and Ports (protocoles et ports). Les politiques créées par l'acceptation d'une demande de politiques couvrant plusieurs portées sont indiquées par un signe Plus à côté du port et du protocole :

Cliquez sur le signe + pour afficher le créateur de la politique transversale et un lien vers la politique consommateur correspondante.

Remarque Les politiques suggérées par la recherche automatique de politiques qui n'ont pas été approuvées peuvent ne pas être présentes après une exécution ultérieure de la recherche de politiques, si les flux de trafic qui les ont produites ne sont pas observés au cours de l'exécution ultérieure. Pour conserver les politiques suggérées, consultez Approuver les politiques, à la page 479.

Examiner et analyser les politiques

Il est essentiel de vous assurer que vos politiques produisent les effets escomptés (et n'ont pas d'effets imprévus) avant de les appliquer.

Consulter les politiques découvertes automatiquement

Passez en revue les résultats de la découverte des politiques sur la page Policies (politiques) de l'espace de travail dans lequel vous avez découvert les politiques.

Commencez votre examen ici

Nous vous recommandons de commencer par vérifier si les politiques traitent de chacun des domaines suivants, dans l'ordre suggéré :

- Ports communs et essentiels
- Trafic Internet

- Trafic entre différentes applications (ces flux peuvent impliquer des charges de travail de différentes portées)
- Trafic au sein de la même application (ces flux sont susceptibles d'impliquer des charges de travail dans la même portée)

Outils utiles pour l'examen des politiques

- Pour faciliter la gestion de cet effort, filtrez et triez les politiques afin de pouvoir examiner les politiques associées en tant que groupe.
  - Cliquez sur les en-têtes du tableau pour trier les colonnes, par exemple par consommateur, fournisseur ou port/protocole.
  - Utilisez le filtre en haut de la liste des politiques pour afficher des sous-ensembles spécifiques.

    Pour afficher la liste des propriétés que vous pouvez filtrer, cliquez sur le bouton (i) dans la zone Filter Policies (Filtrer les politiques).

- Examinez la représentation graphique des politiques générées :

  Cliquez sur le bouton  (bouton d'affichage visuel de la politique).

  Pour en savoir plus, consultez Représentation visuelle des politiques, on page 542.
- Pour rechercher ou filtrer les lignes en fonction des ports, cliquez sur le bouton **Ungrouped** (Dégroupées).
- Par défaut, les politiques sont regroupées par consommateur/fournisseur/action. Pour revenir à cet affichage, cliquez sur le bouton **Grouped** (Groupées).
- Utiliser le filtre **External?** (Externe?) pour trouver les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle dans laquelle vous avez découvert les politiques.

  Créez des politiques pour ce trafic en utilisant l'une des méthodes décrites dans Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques, on page 522.
- Examinez le niveau de confiance des politiques générées. Consultez Traiter les politiques de niveau de confiance faible, on page 540.
- Consultez le profil de charge de travail pour obtenir des renseignements détaillés sur une charge de travail. Cliquez sur l'adresse IP, puis sur **View Workload Profile** (afficher le profil de charge de travail) dans le volet de droite.
- Pour afficher les flux de trafic qui ont été utilisés pour produire une politique spécifique, cliquez sur la valeur dans la colonne **Protocols and Ports** (protocoles et ports) de cette politique, puis cliquez sur **View Conversations** (afficher les conversations) dans le panneau latéral qui s'ouvre.

  Consultez Conversations, on page 581 pour obtenir de plus amples renseignements.

  Si nécessaire, vous pouvez accéder au détail en cliquant sur **Flow Search** (recherche de flux) pour afficher les flux d'une conversation.

Autres choses à faire et à vérifier

- Repérez les adresses IP inconnues (comme les adresses IP de basculement ou autres adresses IP flottantes) et ajoutez-leur des étiquettes pour savoir de quoi il s'agit.

Vous pouvez trouver des détails utiles sur la page Inventory Profile (Profil d'inventaire). Cliquez sur l'adresse IP, puis sur **View Inventory Profile** (afficher le profil d'inventaire) dans le volet de droite.

- Recherchez tout ce qui n'est manifestement pas souhaitable ou qui n'a pas de sens.
- Regroupez les charges de travail à l'aide de filtres d'inventaire pour qu'une seule politique puisse gérer plusieurs d'entre elles. Consultez Créer un filtre d'inventaire, on page 392.
- Enquêtez et contactez d'autres administrateurs réseau, au besoin, pour comprendre la nécessité des politiques que vous voyez.
- Consultez les rubriques sous Aborder les complexités de la politique, on page 515, qui peuvent impliquer des politiques manuelles et approuvées ainsi que des politiques détectées automatiquement.
- En général, il est recommandé que le nombre maximal de politiques d'une portée ne dépasse pas 500 environ. Si vous en avez beaucoup plus, essayez de regrouper des politiques similaires ou de diviser la portée.
- Lors de l'examen, approuvez toutes les politiques dont vous savez qu'elles sont correctes en l'état, afin de les conserver lors de futurs cycles de découverte.

Traiter les politiques de niveau de confiance faible

Après la découverte automatique d'une politique, les indices de confiance indiquent la précision et la pertinence de chaque politique découverte pour chaque service (port et protocole) spécifié dans cette dernière.

Pour identifier les politiques de niveau de confiance faible découvertes :

1. Accédez à la portée et à l'espace de travail applicables, puis cliquez sur **Manage Policies** (Gérer les politiques).
2. Cliquez sur l'onglet **Policies** (Politiques).
3. Cliquez sur le bouton **Ungrouped Policy List View** (Affichage de la liste des politiques non groupées).
4. Cliquez sur l'en-tête de colonne **Confidence** (Confiance) pour trier la liste des politiques par niveau de confiance.
5. Cliquez sur la valeur dans la colonne **Protocols and Ports** (Protocoles et ports) pour ouvrir un volet dans la partie droite de la fenêtre.
6. Dans la section **Protocols and ports** (Protocoles et ports), la couleur de chaque **C** indique le niveau de confiance pour chaque service (port et protocole) spécifié dans la politique.

   Pour interpréter le niveau de confiance, survolez le **C**.
7. Recherchez les indicateurs de niveau de confiance faible pour tous les services de la liste.
8. Le cas échéant, supprimez ou modifiez les politiques indésirables ou ajoutez des politiques supplémentaires.

Pour afficher les niveaux de confiance d'une politique particulière :

1. Dans l'onglet Policies (politiques), cliquez sur la valeur de la colonne **Protocols and Ports** (protocoles et ports) pour cette politique.

   Le panneau d'affichage latéral des politiques s'ouvre dans la partie droite de la fenêtre.

2. Dans la section **Protocols and ports** (Protocoles et ports), la couleur de chaque **C** indique le niveau de confiance pour chaque service (port et protocole) spécifié dans la politique.

   Pour interpréter le niveau de confiance, survolez le **C**.

Direction du flux et niveau de confiance de la politique

La précision des politiques détectées dépend de l'identification correcte de la direction du flux. Si la direction du flux est mal identifiée, le degré de confiance des résultats de la recherche automatique de politiques peut être diminué. Pour en savoir plus sur la détermination de la direction du flux pour la ou les conversations analysées pour la création de la politique, consultez Classification client-serveur.

Dépanner les résultats de la découverte automatique des politiques

Si les résultats de la découverte automatique des politiques ne sont pas conformes à vos attentes, vérifiez les points suivants :

Étendre la plage temporelle sélectionnée pour inclure plus de données

Prolonger la fenêtre temporelle pour inclure davantage de données et pour incorporer les événements qui se produisent rarement. Par exemple, si une application génère un rapport trimestriel complexe à partir de données provenant de plusieurs applications de fournisseurs, veillez à inclure une plage temporelle qui inclut ce trafic.

Éviter les données recueillies avant certaines modifications

Si la définition de la portée a été modifiée ou si des données recueillies avant un certain moment sont devenues non valides pour une autre raison, assurez-vous que votre plage temporelle n'inclut PAS de données antérieures.

Exclure les flux de trafic trompeurs

Les filtres d'exclusion doivent peut-être être configurés ou modifiés.

Les filtres d'exclusion peuvent être configurés à plusieurs endroits, ils peuvent être activés ou désactivés. Vérifiez chaque emplacement :

- Vérifiez les filtres d'exclusion configurés pour l'espace de travail.
- Vérifiez les filtres d'exclusion par défaut configurés au bas de la page de configuration de la découverte de la politique par défaut.
- Vérifiez quels filtres d'exclusion sont activés dans la section Advanced Configurations (configurations avancées) des paramètres de l'espace de travail pour la découverte automatique des politiques.
- Vérifiez quels filtres d'exclusion sont activés dans la section Advanced Configurations (configurations avancées) de la page de configuration de la découverte des politiques par défaut.
- Si vous utilisez des filtres d'exclusion par défaut, assurez-vous d'avoir cliqué sur **Save** (Enregistrer) dans la page **Default Policy Discovery Config** (configuration de la découverte de politiques par défaut) pour rendre ces configurations disponibles pour les espaces de travail individuels.

Pour en savoir plus, consultez Filtres d'exclusion, à la page 459 et les sous-sections.

Dépannage des politiques selon lesquelles le consommateur et le fournisseur se trouvent dans des portées différentes

Consultez Dépannage des politiques de portées croisées, à la page 534.

Vérifier l'état des politiques approuvées

Consultez Dépanner les politiques approuvées, à la page 480.

Représentation visuelle des politiques

La représentation visuelle des politiques fournit une représentation graphique de ces dernières.

Pour accéder à la page de représentation visuelle des politiques : Dans la page Policies (Politiques), cliquez sur l'icône de graphique () à droite de l'icône de liste.

Éléments d'affichage de la politique

Les éléments visuels de la vue des politiques sont les suivants :

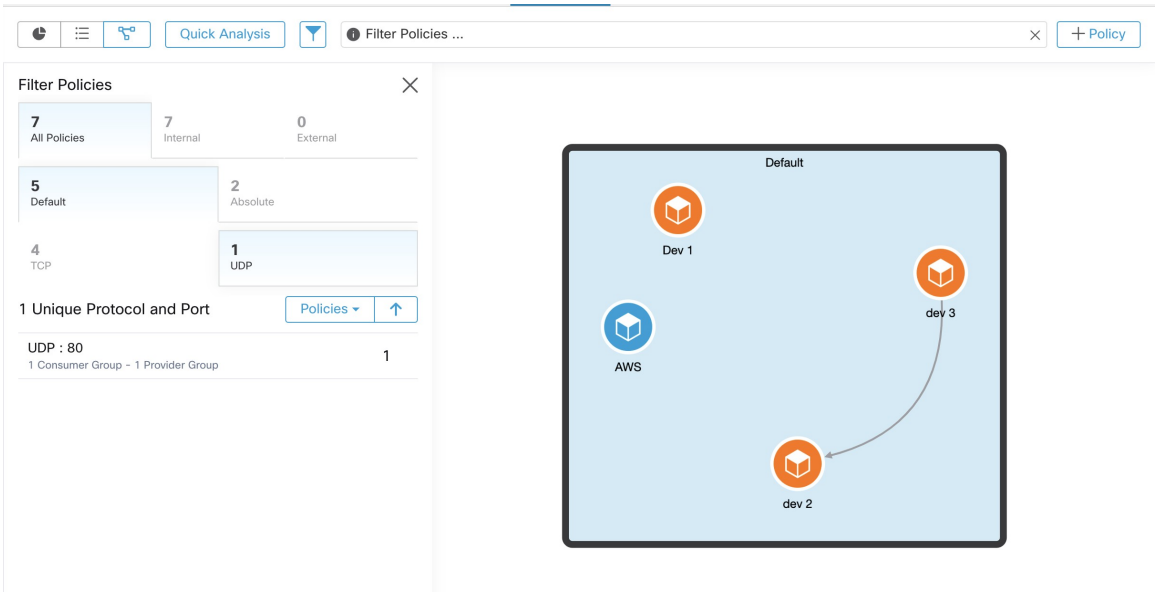
Cet élément	Représente
Une icône bleue, orangée ou mauve	Un nœud (le consommateur ou le fournisseur d'une politique)
Icône bleue	Une portée
Icône jaune	Un filtre d'inventaire
Icône mauve	Une grappe
Ligne reliant deux icônes	Une ou plusieurs politiques

Options d'affichage des politiques

Destinataire	Faire ceci
Afficher la liste des charges de travail incluses dans un nœud de consommateur ou de fournisseur	Double-cliquez sur l'icône du nœud.
Afficher les détails d'une politique telles que les services (ports), les actions (autoriser/refuser) et le protocole entre un consommateur et un fournisseur	Double-cliquez sur la ligne qui les relie. Les détails s'affichent dans le volet de droite.
Afficher les politiques entrant et sortant d'un nœud	Cliquez sur l'icône .
Afficher uniquement les politiques entre les charges de travail de la portée	Cliquez sur le bouton **interne**.
Afficher uniquement les politiques dans lesquelles le fournisseur se trouve dans une portée différente de celle du consommateur	Cliquez sur le bouton **externe**.

Destinataire	Faire ceci
Utiliser les options avancées	Cliquez sur le bouton (i) à gauche de la zone de saisie de texte du filtre pour voir les options, puis saisissez les critères de filtre.

Figure 299: Filtrage des politiques dans la vue graphique



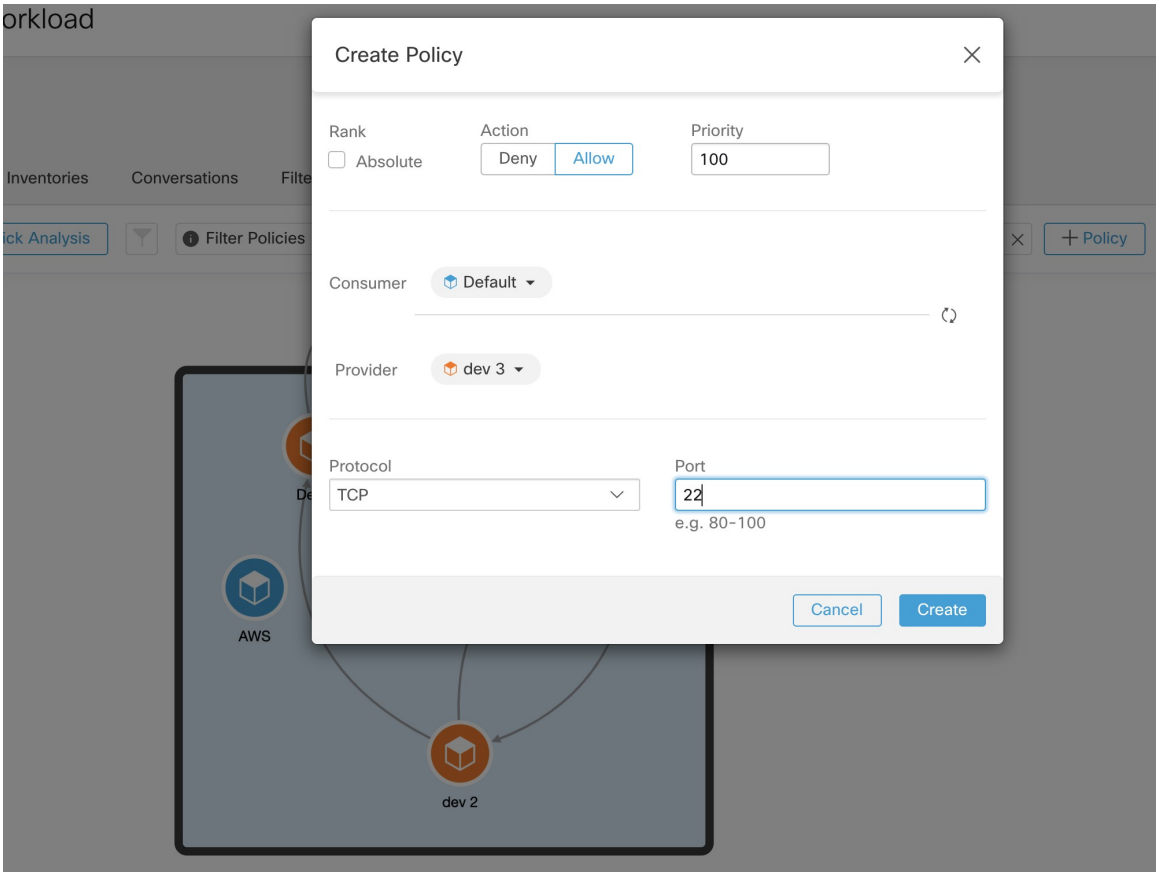
Pour télécharger une image haute résolution de la vue graphique des politiques :

1. Dans le coin inférieur droit du graphique, cliquez sur l'icône de points de suspension , puis cliquez sur **Export Image** (Exporter l'image).
2. Sélectionnez la résolution et le type d'image requis.
3. Cliquez sur **Télécharger**.

Ajouter une politique (page d'affichage des politiques)

Pour créer une politique, survolez le consommateur jusqu'à ce que vous voyiez un signe « + », puis maintenez la politique enfoncée et faites glisser la politique sur le fournisseur. Pour créer une politique Absolue, cochez la case Absolue dans la boîte de dialogue modale. Sinon, la politique est créée en tant que politique par défaut. Les politiques peuvent également être gérées en cliquant sur une ligne et en sélectionnant une politique dans la liste contextuelle. Les politiques seront affichées dans la barre latérale.

Figure 300: Création de politiques dans la vue graphique



Analyse rapide

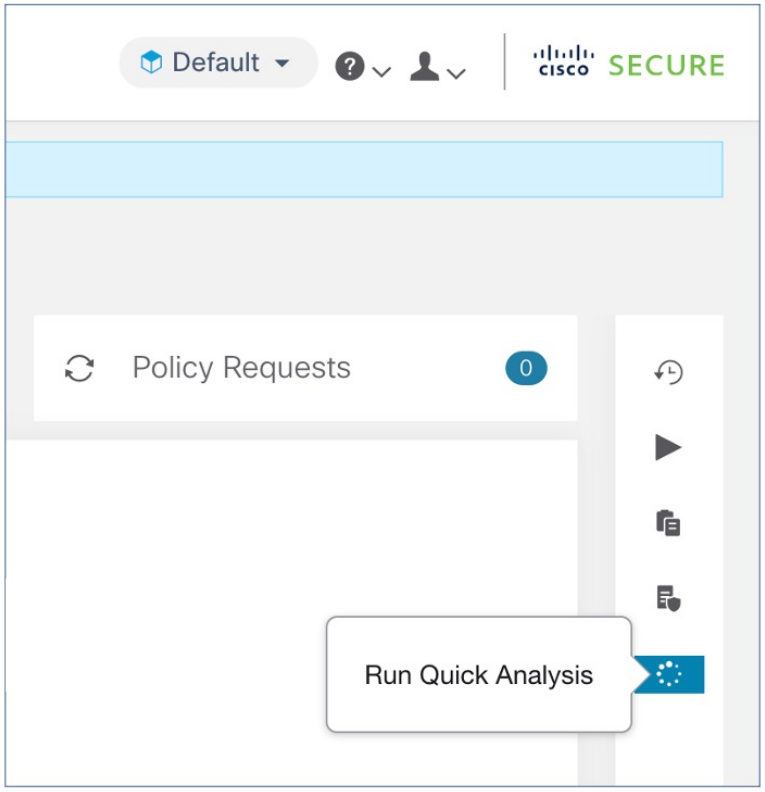
L'analyse rapide permet de tester un flux au sujet duquel on a des doutes par rapport à toutes les politiques de l'espace de travail actuel et à toutes les autres politiques pertinentes d'autres espaces de travail. L'analyse rapide facilite le débogage et l'expérience de différentes politiques de sécurité, sans qu'il soit nécessaire d'exécuter une analyse des politiques en direct pour l'espace de travail.

Restriction

- Vous ne pouvez exécuter l'analyse rapide que sur les espaces de travail principaux.
- L'analyse rapide n'est actuellement pas prise en charge sur les flux des services Kubernetes.

Cliquez sur l'onglet **Run Quick Analysis** (Exécuter l'analyse rapide) dans le volet de navigation de droite pour afficher la boîte de dialogue.

Figure 301: Onglet Analyse rapide



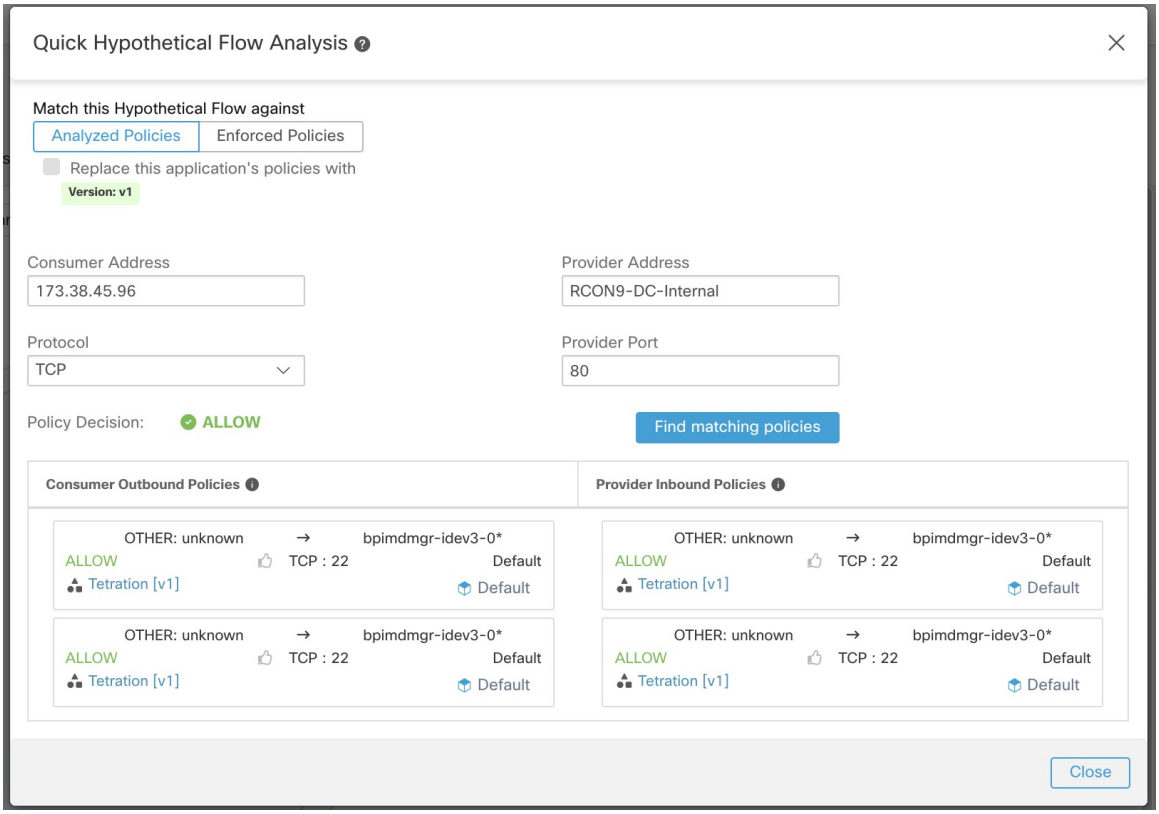
Saisissez l'adresse IP du consommateur (client), l'adresse IP du fournisseur (serveur), le port et le protocole du flux hypothétique, puis cliquez sur le bouton **Find Matching Policies** (trouver les politiques correspondantes).

Une décision de politique sera affichée, indiquant si le flux hypothétique serait autorisé ou refusé compte tenu des définitions de politique de la dernière version de l'espace de travail et de toutes les autres politiques pertinentes des espaces de travail qui sont déjà transmises pour l'analyse de politique en direct.

Au bas de la boîte de dialogue, nous affichons les politiques sortantes et entrantes correspondantes séparément, et dans leur ordre de tri global. Seule la première rangée de chaque côté a un effet. Pour qu'une connexion soit établie avec succès, nous avons besoin que la règle de trafic sortant sur le consommateur et la règle entrante supérieure du côté du fournisseur soient des règles ALLOW.

L'affichage de toutes les autres politiques correspondantes dans l'ordre fournit un outil de débogage précieux pour aider à résoudre les problèmes dans les définitions de politiques lorsqu'une certaine politique semble ne pas avoir d'effet. Vous pouvez ajouter, mettre à jour ou supprimer des politiques de l'espace de travail et répéter immédiatement l'analyse sans avoir à exécuter une analyse des politiques en direct sur l'espace de travail.

Figure 302: Analyse rapide de la politique



Analyse des politiques en temps réel

Après avoir examiné et approuvé l'ensemble de politiques de sécurité de réseau généré par la découverte automatique des politiques et avant d'appliquer les politiques, vous devez utiliser l'analyse des politiques en direct pour observer comment les politiques pourraient affecter le trafic réel sur votre réseau.

Voici des questions auxquelles l'analyse des politiques en temps réel peut vous aider à répondre :

- Quelle serait l'incidence sur les applications de cette portée si les politiques de cet espace de travail étaient appliquées maintenant?
- Aurait-on pu éviter une attaque ou un risque de sécurité connu précédemment en appliquant le nouvel ensemble de politiques?

  Consultez Exécuter des expériences de politiques pour comparer les politiques actuelles au trafic passé, on page 554.

- Nos politiques fonctionnent-elles comme nous l'attendons?

Vous devez exécuter l'analyse des politiques sur tout espace de travail qui comporte des politiques. Étant donné que les charges de travail d'une portée spécifique peuvent être affectées par des politiques d'autres portées, vous ne devez pas exécuter l'analyse des politiques uniquement pour une portée unique avant d'appliquer la politique pour cette portée. Pensez à analyser les politiques de toutes les portées qui peuvent avoir une incidence sur le trafic d'une portée particulière.

Par exemple :

- Les politiques définies dans les portées supérieures à cette portée dans l'arborescence peuvent s'appliquer aux charges de travail de cette portée.
- Si les charges de travail de cette portée communiquent avec des charges de travail d'une autre, les politiques de cette portée peuvent affecter ces communications. Lorsque l'analyse des politiques est lancée dans cette portée (ou que les dernières politiques sont analysées après un changement de politique dans cette portée), cela peut affecter les résultats de l'analyse des politiques de cette portée.

Vous devez effectuer une analyse des politiques chaque fois que vous les mettez à jour pour vous assurer que les modifications n'endommagent pas les applications.

L'exécution d'une analyse des politiques en temps réel sur un espace de travail est parfois appelée « publication » d'un espace de travail.

Commencer l'analyse des politiques en temps réel

Une fois que vous avez examiné les politiques générées dans un espace de travail par la découverte automatique des politiques et que vous pensez qu'elles sont telles que vous le souhaitez, vous pouvez commencer leur analyse.

Before you begin

Important L'analyse en temps réel comprend les effets des politiques dans d'autres espaces de travail qui exécutent également l'analyse en direct. Si vous avez activé la mise en application sur un espace de travail, mais que l'analyse n'est pas en cours sur cet espace de travail ou que la version appliquée des politiques n'est pas la même que la version analysée des politiques, les résultats de l'analyse en temps réel pour cet espace de travail risquent de ne pas être exacts.

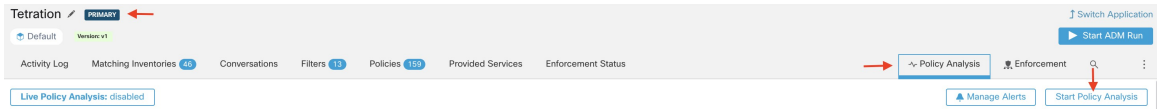
Procedure

Étape 1 Basculez l'espace de travail sur **Primary** (Principal) en cliquant sur le bouton ••• (bouton Plus) à droite de « Secondary » (Secondaire) à côté du nom de l'espace de travail dans l'en-tête.

Étape 2 Accédez à l'onglet **Policy Analysis** (analyse des politiques).

Étape 3 Cliquez sur **Start Policy Analysis** (Démarrer l'analyse des politiques) sur la droite.

Figure 303: Activer l'analyse des politiques



What to do next

- Étant donné que les politiques d'autres portées peuvent s'appliquer aux charges de travail de cette portée, envisagez d'analyser simultanément les politiques d'autres portées qui pourraient affecter les résultats de

l'analyse de cette dernière.. Consultez Exemple : Incidence des politiques analysées sur d'autres portées, on page 549.

- Si vous souhaitez être averti lorsque des flux échappés sont détectés, cliquez sur **Manage Alerts** Gérer les alertes).
- Utilisez les outils de la page pour filtrer les données. Pour afficher les critères de filtre disponibles, cliquez sur le bouton (i) dans la zone de filtre.
- Si vous ajoutez ou modifiez des politiques après avoir lancé l'analyse, vous devez redémarrer l'analyse pour inclure les modifications dans cette dernière. Consultez Après avoir modifié les politiques, analyser les dernières politiques, on page 555.

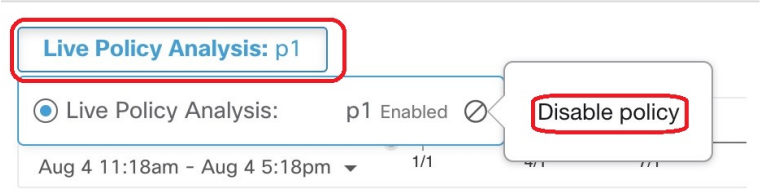
Arrêter l'analyse des politiques en direct

En général, vous devez laisser l'analyse des politiques continuer de s'exécuter, même après l'application des politiques, car les politiques de cet espace de travail peuvent avoir une incidence sur les résultats de l'analyse des politiques dans d'autres espaces de travail que vous analysez.

Pour arrêter l'analyse des politiques en direct :

Cliquez sur **Live Policy Analysis : P<number>**(Analyse de la politique en direct), puis cliquez sur **Disable Policy** (désactiver la politique) :

Figure 304: Désactiver l'analyse en temps réel des politiques

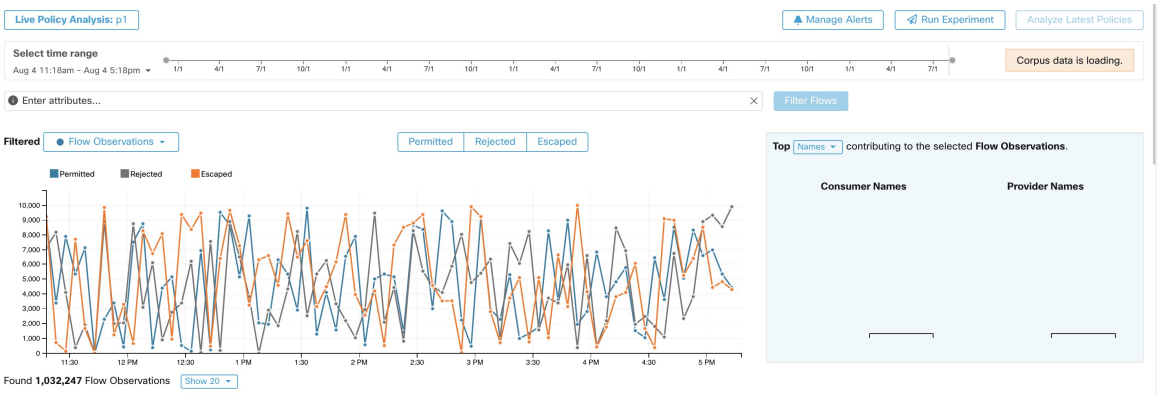


Résultats de l'analyse des politiques : comprendre les bases

Lors de l'analyse de la politique, tous les flux entrant, sortant et se trouvant dans la portée associée à l'espace de travail se voient attribuer l'un des résultats suivants :

- **Autorisé** : le flux a été autorisé par le réseau ainsi que par les politiques analysées.
- **Échappé** : le flux a été autorisé par le réseau, mais aurait dû être abandonné selon les politiques analysées.
- **Rejeté** : le flux a été abandonné par le réseau, ainsi que par les politiques analysées.

Figure 305: Page Policy Analysis (Analyse de la politique)



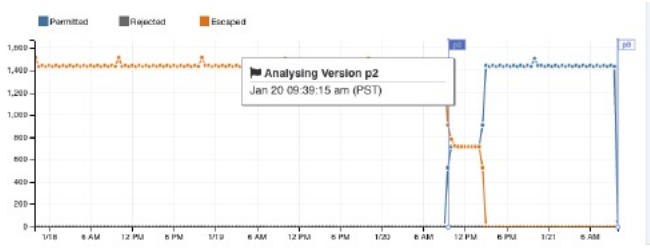
Quelques éléments à prendre en considération pour s'orienter :

- Vous pouvez filtrer les renseignements sur les flux présentés dans cette page à l'aide d'une barre de filtre à aspects multiples. Cliquez sur le bouton **Filter Flows** (Filtrer les flux) pour mettre à jour tous les graphiques en conséquence.
- Passez la curseur sur le graphique pour afficher le pourcentage des flux agrégés observés lors de cet horodatage.
- Cliquez sur un horodatage pour afficher une liste de tous les flux filtrés dans un tableau ci-dessous pour une analyse plus approfondie.
- Vous pouvez limiter les interactions à l'un des trois types de résultats en cochant ou en décochant les types en haut des graphiques de séries temporelles.
- Le tableau intitulé Top N (à droite) montre les principaux noms d'hôte, adresses, ports, etc. qui contribuent aux données présentées dans la série temporelle à gauche.

  Vous pouvez limiter le tableau des séries temporelles aux flux échappés et sélectionner « Ports » dans le tableau des N principaux pour voir les principaux ports qui contribuent aux flux échappés.

Exemple : Incidence des politiques analysées sur d'autres portées

Dans l'exemple suivant, les flux sont autorisés jusqu'à environ 12 h. À ce moment-là, l'analyse des politiques a été lancée dans un espace de travail associé à une portée différente, affectant le trafic avec des charges de travail dans cette portée et entraînant le marquage des flux comme échappés. (Vous savez que cette modification ne résultait pas de modifications de politique nouvellement analysées dans cet espace de travail, car cela aurait créé un indicateur d'étiquette).



Analyse sans politiques

Les flux entrants, sortants et à l'intérieur de la portée associée à l'espace de travail peuvent être affectés par les politiques d'autres espaces de travail en cours d'analyse. Si l'analyse des politiques en direct n'est pas activée dans cet espace de travail, les flux seront marqués avec ceux des autres espaces de travail du système dans lesquels l'analyse des politiques en direct est activée.

Note Si aucun espace de travail n'exécute d'analyse de politique en direct, le graphique de la série chronologique est vide.

Détails de l'analyse de la politique

Disposition des flux

Dans l'analyse en direct des politiques, pour décider si un flux est **autorisé**, **échappé** ou **rejeté**, nous devons d'abord déterminer la **disposition** du flux du point de vue du réseau. Chaque flux recevra la disposition **ALLOWED (AUTORISÉ)**, **DROPPED (ABANDONNÉ)** ou **PENDING (EN ATTENTE)** , en fonction des signaux et des observations donnés par les agents Cisco Secure Workload. Il existe un certain nombre de scénarios basés sur les configurations des agents le long du chemin du flux et des types de flux.

Tout d'abord, quels que soient les types de flux, si un agent sur le chemin d'un flux signale que le flux est ABANDONNÉ, ce flux recevra le statut ABANDONNÉ.

Lorsqu'aucun agent ne signale d'ABANDON le long du chemin du flux, nous considérons le cas des flux bidirectionnels et unidirectionnels séparément. Lorsque des flux bidirectionnels sont observés, nous examinons les flux par paires (aller et retour) en fonction de leur source, de leurs ports et protocoles de destination et de leur synchronisation. On ne peut pas faire de même pour les flux unidirectionnels.

Pour les flux bidirectionnels, si des agents sont installés et le plan de données activé aux deux extrémités, un flux aller recevra une disposition AUTORISÉE si l'agent de source et l'agent de destination indiquent que le flux est observé. Sinon, le flux aller aura la disposition PENDING (EN ATTENTE). Si un agent est installé sur la charge de travail source ou de destination, mais pas sur les deux, le flux aller recevra une disposition AUTORISÉE si et seulement si l'agent observe le flux inverse ultérieur durant une fenêtre de **60** secondes Sinon, l'état PENDING (EN ATTENTE) sera attribué au flux aller. La disposition de la partie inverse du flux bidirectionnel suit la même logique, sauf que maintenant la source et la destination sont inversées. Par exemple, si un seul côté comporte un agent, le fait qu'une disposition de flux inverse soit EN ATTENTE ou AUTORISÉ dépend de l'observation et du moment de son flux aller suivant selon la même logique.

Notez que nous supposons que les pare-feu mettent en œuvre la suppression silencieuse. Si un message de rejet est envoyé sur le *même* flux (par exemple, le rejet d'un SYN TCP avec RST + ACK), un flux inverse sera détecté et le flux aller précédent sera marqué comme AUTORISÉ. Cependant, si le message de rejet est envoyé sur un flux *différent* (par exemple, rejet d'un message SYN TCP avec un message ICMP), le flux aller restera PENDING (EN ATTENTE).

Pour un flux unidirectionnel, le flux sera considéré comme ABANDONNÉ s'il est signalé comme ABANDONNÉ par un agent, comme dans le cas des flux bidirectionnels. Cependant, comme il n'y a pas de flux inverse correspondant, le flux aura l'état de disposition PENDING (EN ATTENTE) si les deux agents l'observent.

Types de violations

Les dispositions de flux sont vérifiées par rapport aux politiques analysées pour déterminer les types de violation finaux.

Le type de violation d'un flux sera

- **Permitted (Autorisé)**, si sa disposition est ALLOWED ou PENDING et que son action politique décisionnelle est ALLOWED,
- **Escaped (Échappé)**, si sa disposition est ALLOWED et que son action politique décisionnelle est DENY,
- **Rejected (Rejeté)** , si sa disposition est DROPPED ou PENDING et que son action politique décisionnelle est DENY,

Un état DROPPED est attribué uniquement aux flux dont les agents concernés signalent explicitement leur état ABANDONNÉ. En l'absence de rapport explicite d'abandon pour les agents, le flux reçoit l'état PENDING (EN ATTENTE).

Lorsque la disposition est PENDING (EN ATTENTE) :

- et que l'action de la politique est DENY (REJETER), le type de violation est défini sur Rejeté.
- et que l'action de la politique est ALLOWED (AUTORISÉ), le type de violation est réglé sur Autorisé.

Dans un flux bidirectionnel, si les types de violation de politique aller et retour du flux concordent, un seul type s'affiche dans l'analyse des politiques ou dans la page d'analyse de l'application. Sinon, le trajet avant et arrière sont affichés séparément, par exemple ALLOWED:REJECTED.

Exemples de scénarios :

- Des paquets sont abandonnés au niveau de l'application côté source.
  - Dans ce cas, l'agent de sortie Cisco Secure Workload du côté source signalera que le flux est ABANDONNÉ.
- Des paquets quittent la source.
  - S'il n'y a qu'un agent du côté source, le flux sera signalé comme AUTORISÉ par l'agent de sortie si un retour de paquet est également observé par l'agent dans les 60 secondes.
  - S'il y a un agent de visibilité seulement du côté de la source et du côté de la destination, le flux recevra l'état de disposition ABANDONNÉ si et seulement si l'agent d'entrée signale que le flux est ABANDONNÉ. Sinon, le flux sera signalé comme AUTORISÉ.
  - Des paquets de flux sont reçus à destination, mais pas de trafic inverse.

    S'il n'y a pas d'agent du côté destination, le flux recevra l'état PENDING (EN ATTENTE). Sinon, le statut AUTORISÉ lui sera attribué.

Étapes suggérées pour l'analyse des flux

Lors de l'analyse de flux spécifiques lors de l'examen des résultats des politiques, les suggestions et les filtres suivants peuvent être utiles :

1. Concentrez-vous d'abord sur les *FLUX ÉCHAPPÉS* :

   Les flux **échappés** nécessitent une attention particulière, car leurs dispositions réelles de flux diffèrent des actions prévues en fonction des politiques actuellement analysées. Vérifiez que l'application de ces politiques ne bloque pas les flux nécessaires et ne nuit pas à vos applications.

   Cliquez sur le type de violation, par exemple **Échappé**.

(Vous pourrez ultérieurement consulter les flux rejetés et autorisés, si nécessaire).

Les flux échappés peuvent se produire pour de nombreuses raisons, notamment :

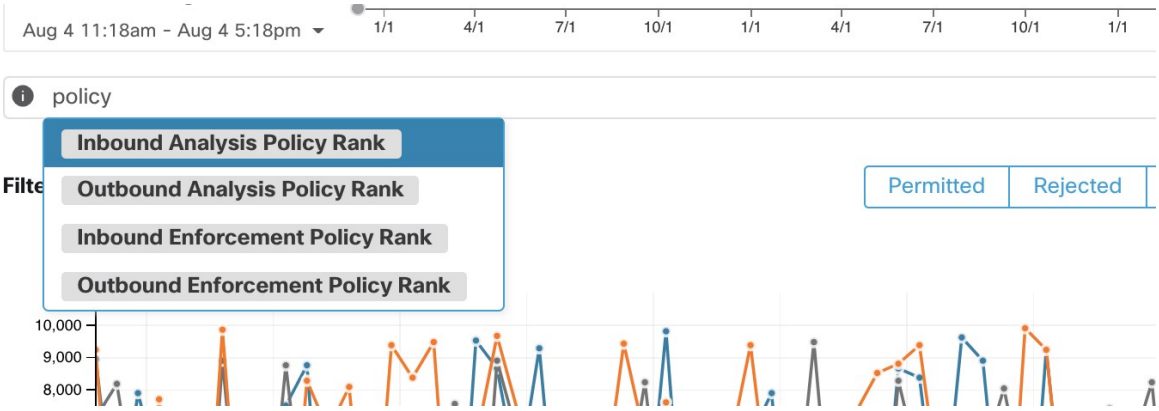
- Une autre politique plus élevée dans l'ordre de priorité est en train de prendre effet
- le trafic emprunte un chemin différent du chemin de routage indiqué par vos politiques, ou
- Par exemple, la politique que vous attendez du trafic se trouve dans un espace de travail qui n'est pas analysé (si vous regardez les flux échappés sur la page Analyse de la politique) ou mis en application (si vous regardez les flux échappés sur la page Application), par exemple dans une portée ancêtre ou même dans un espace de travail secondaire dans la même portée.

2. Identifier les flux qui correspondaient à la politique collectrice globale (entrants et sortants) :

   Il est important de comprendre quels flux sont associés aux politiques collectrices globales, en particulier dans un modèle de politique de liste d'autorisation. Si ces flux sont légitimes, mais qu'aucune politique d'autorisation explicite n'est configurée pour eux, vous pouvez ajouter des politiques explicites appropriées dans les portées entrantes ou sortantes correspondantes. S'il s'agit de flux suspects, vous devez les identifier rapidement et étudier plus avant leurs détails.

   Pour vous concentrer sur ces flux, appliquez des filtres en fonction de la valeur *catch-all* (collectrice globale) de **inbound_policy_rank** ou **out- bound_policy_rank**, selon que vous examinez le flux entrant, sortant ou les deux, comme indiqué ci-dessous.

   Illustration 306 : Options de filtrage de l'analyse des politiques pour le classement



3. Filtrer les flux TCP avec RST : *les indicateurs Fwd (Avant) ne contiennent pas RST, les indicateurs Rev (Retour) ne contiennent pas RST*

   Certains flux TCP échappés ont des indicateurs RST activés. Ces flux sont réinitialisés par leurs consommateurs ou leurs fournisseurs. Il s'agit de connexions non établies sans échange de données, mais qui peuvent être signalées comme AUTORISÉES, car les agents peuvent voir leurs paquets d'établissement de liaison. Puisque ces flux n'ont pas de connexions établies pour commencer, ils ne seront pas affectés lors de l'application des politiques actuellement analysées. Le filtrage des flux TCP qui ont l'indicateur RST de chaque côté vous permet de vous concentrer sur les flux échappés plus significatifs et plus importants, dont la connexion établie sera bloquée par les politiques actuellement analysées.

4. Si la majeure partie du trafic utilise IPv4, concentrez-vous uniquement sur les flux IPv4 :

   Filtre utilisant *address type = IPv4, address type != IPv6*. Il est également utile de filtrer les adresses *link-local* (liées locales).

5. Hiérarchisez les flux sur lesquels se concentrer lors de la prochaine étape de diagnostic en identifiant les noms d'hôte, les ports, les adresses, les portées, etc. les plus fréquemment concernées par le trafic échappé :

   Sélectionnez le *nom d' hôte, les ports ou* les *adresses* dans le volet de fonctionnalité TopN. Vous pouvez généralement les combiner avec d'autres filtres pour accéder à un type de trafic particulier lors du diagnostic des politiques.

6. Rechercher les données de flux pour les noms d'hôte, les ports, les protocoles, etc., identifiés à l'étape précédente

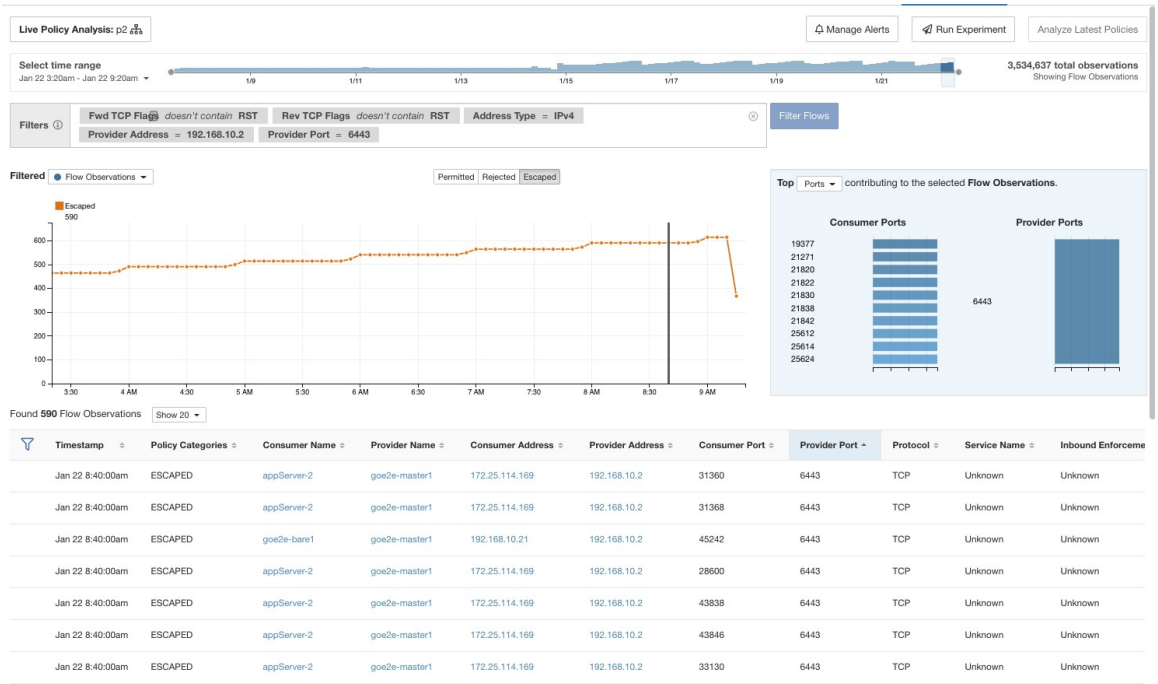
   Une fois que vous avez une idée des principaux candidats en fonction des noms d'hôte, de port, etc. des flux ciblés, vous pouvez choisir d'approfondir les flux en appliquant des filtres d'exploration directement à partir des N premières valeurs données dans la fenêtre de requête N supérieure, ou en saisissant manuellement les filtres pertinents dans la barre des filtres de recherche de flux. Par exemple, *Consumer Hostname contains {something}, Provider Hostname contains {something}, Provider Port = {some port number}, Protocol = TCP Protocol != ICMP*

7. Consultez les flux individuels et effectuez une analyse rapide :

   Enfin, vous pouvez vous concentrer sur un flux en particulier pour examiner le résultat de ses politiques en cliquant sur la ligne du tableau correspondant au flux. Soyez attentif aux politiques correspondant au flux et aux portées des adresses du consommateur et du fournisseur. Si l'action de politique ne correspond pas à l'action prévue, vous devez créer des politiques appropriées dans les espaces de travail associés aux portées du fournisseur et/ou du consommateur pour modifier l'action de la politique.

   La figure ci-dessous montre un exemple de flux de travail de réduction des flux échappés à l'aide du filtrage décrit ci-dessus. L'entrée de recherche prend également en charge les « , » et « - » pour le port, l'adresse du consommateur et l'adresse du fournisseur, en transformant les « - » en requêtes de plages.

Illustration 307 : Exemple de diagnostic d'analyse de politiques



Exécuter des expériences de politiques pour comparer les politiques actuelles au trafic passé

Si une attaque connue ou un autre modèle de trafic important à court terme s'est produit par le passé, et vous souhaitez voir comment vos politiques actuelles (ou un autre ensemble de versions de politiques) auraient géré ce trafic, vous pouvez utiliser la fonctionnalité Run Experiments « exécuter des tests ».

Before you begin

Tip Au lieu de cette procédure, vous pouvez exécuter à nouveau la découverte automatique des politiques, y compris la plage temporelle pertinente, et voir quelles politiques différentes sont suggérées.

Procedure

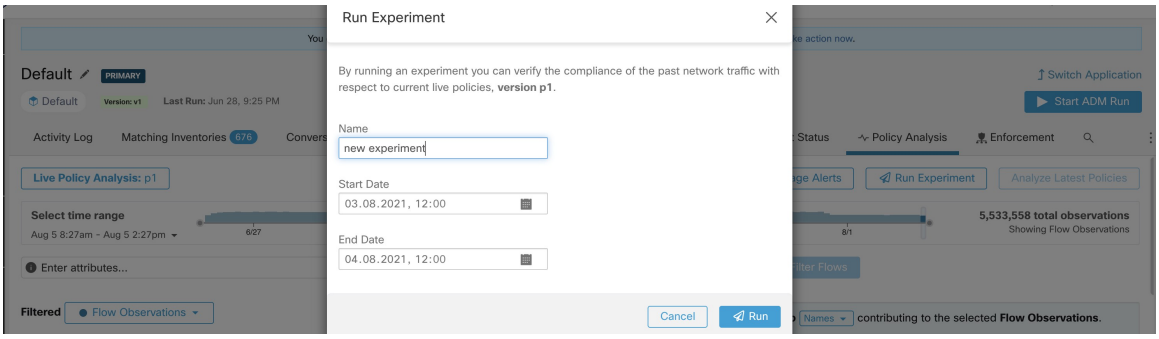
Étape 1 Accédez à la page d'analyse des politiques de votre espace de travail sélectionné.

Étape 2 En haut de la page, sélectionnez la version de la politique à tester.

Étape 3 Cliquez sur **Run Experiment** (Exécuter l'expérience).

Étape 4 Saisissez un nom et une durée pour le test de la politique.

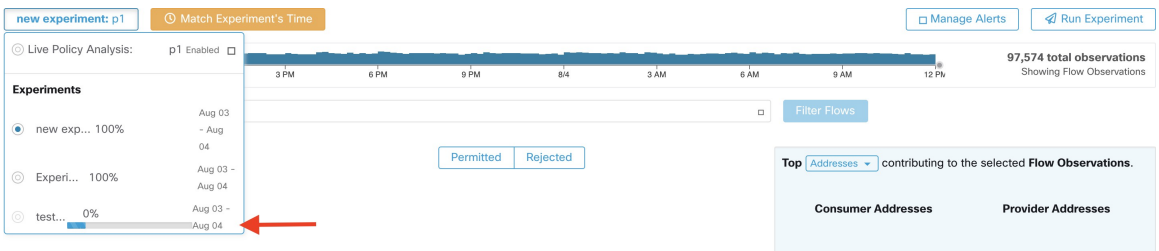
Figure 308: Exécuter le formulaire de test



Cette opération lance un nouveau travail d'analyse de la politique qui remonte dans le temps et réanalyse tous les flux de la durée sélectionnée en fonction dans la version de la politique sélectionnée.

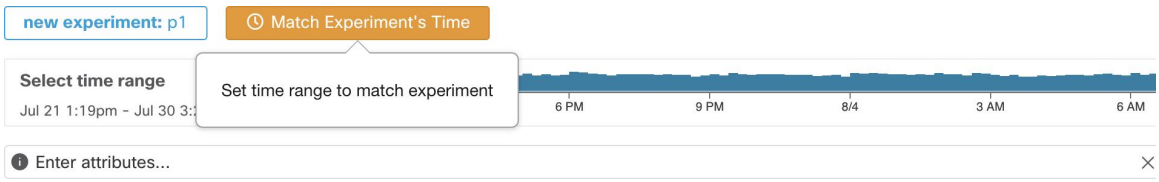
Cette tâche peut prendre quelques minutes, selon la durée sélectionnée. La progression est affichée dans le menu du sélecteur de politiques. Lorsque les résultats sont prêts à être présentés, vous devriez pouvoir sélectionner l'expérience comme n'importe quelle autre version de la politique et les graphiques de séries temporelles montrant les différentes catégories de flux seront mis à jour en conséquence.

Figure 309: Afficher l'état du test



Note Si vous ne voyez aucun flux lors de la sélection d'une expérience de politique, cela peut être dû à une inadéquation de l'intervalle de temps. Par exemple, l'intervalle de temps actuel des graphiques est d'une heure, mais la durée de l'expérience est de 6 heures dans le passé. Pour réinitialiser la plage temporelle à la durée de l'expérience, cliquez sur l'icône d'horloge à côté du sélecteur de politique.

Figure 310: Plage temporelle de la correspondance



Après avoir modifié les politiques, analyser les dernières politiques

L'analyse des politiques ne reflète pas automatiquement les modifications de politique dans l'espace de travail. Lorsque vous êtes prêt à analyser l'ensemble actuel de politiques après avoir apporté vos modifications, cliquez sur **Analyze Latest Policies** (Analyser les politiques les plus récentes) pour que l'analyse des politiques reflète les modifications.

Si les politiques de l'espace de travail n'ont pas changé depuis le dernier lancement de l'analyse de politiques ou si l'analyse de politiques n'est pas actuellement activée, le bouton Analyze Last Policies (Analyser les politiques les plus récentes) n'est pas disponible. Si le bouton est cliquable, certaines modifications de politique n'ont pas encore été incluses dans l'analyse.

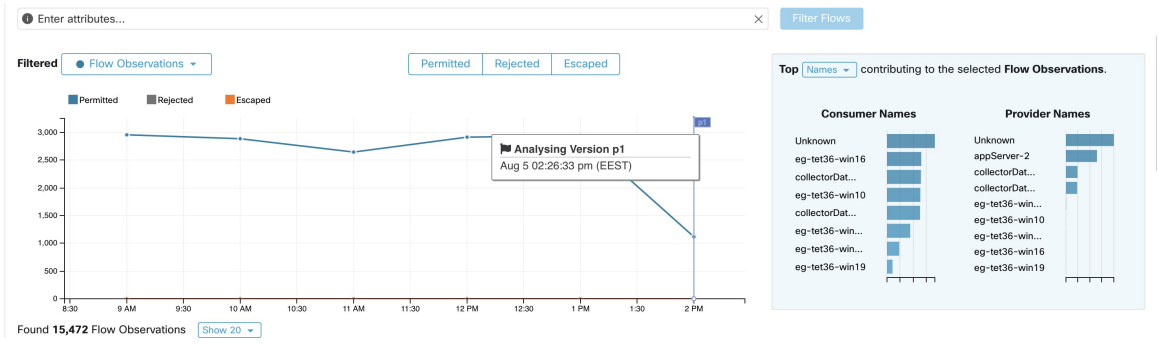
Consultez aussi Afficher, comparer et gérer les versions des politiques analysées, on page 556.

Indicateurs d'étiquette de politique

Sur le graphique de la série chronologique d'analyse des politiques, les indicateurs d'étiquettes de politique marquent le moment où l'analyse a été lancée et à chaque moment l'analyse a été redémarrée pour refléter les dernières modifications de politique et de grappe.

Cliquez sur un indicateur pour afficher la version des politiques associées à cet indicateur :

Figure 311: Indicateur d'étiquette de politique dans le graphique de série chronologique



Cliquer sur un indicateur d'étiquette de politique pour ouvrir la version correspondante de la page Policies (Politiques) et afficher les politiques analysées par cette version d'analyse de politiques.

Afficher, comparer et gérer les versions des politiques analysées

Chaque fois que vous analysez ou réanalysez les politiques dans un espace de travail après avoir apporté des modifications, une nouvelle version d'analyse (p*) est créée.

Pour en savoir plus sur la gestion des versions, consultez À propos des versions des politiques (v* et p*), à la page 575.

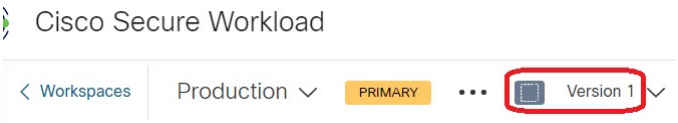
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez au portée et à l'espace de travail principal appropriés.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 La version actuellement affichée des politiques est indiquée en haut de la page :



La version affichée peut être une version de découverte de politique, une version de politique analysée ou une version de politique appliquée.

Étape 5 Vous pouvez réaliser les actions suivantes :

Pour afficher une version différente des politiques :	Cliquez sur la version actuelle et choisissez une version différente. Pour obtenir une description des versions, consultez À propos des versions des politiques (v* et p*), à la page 575. **Important!** Si vous choisissez la version av*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 483 au lieu de cette rubrique, sans oublier la mise en garde importante à la fin de celle-ci.
Pour afficher les détails des versions analysées :	1. Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. 2. Cliquez sur l'onglet **Published Versions** (Versions publiées) pour voir les versions des politiques analysées et appliquées. 3. Pour afficher les entrées de journal pour une version, cliquez sur le lien dans la version. Les lignes vert clair représentent l'activité d'analyse. Les lignes vert clair représentent l'activité d'application de la politique.

Pour comparer deux versions et voir ce qui a changé :	**1.** Cliquez sur **Compare Revisions** (Comparer les révisions). **2.** Choisissez les versions à comparer. Vous pouvez comparer la dernière version provisoire, les versions analysées et appliquées. **3.** Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 577.
Pour supprimer une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Les versions de politique publiées (versions p*) peuvent être supprimées tant que la version n'est pas analysée ou appliquée activement.
Pour exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...).. Consultez aussi Exporter un espace de travail, à la page 487.

Prochaine étape

Lorsque vous avez terminé de travailler avec les versions, remplacez la version en haut de la page de l'espace de travail par la dernière version de politique découverte (v*).

Cela évite la suppression involontaire des versions de politiques découvertes et vous permet de créer manuellement des politiques dans l'espace de travail.

Journaux d'activité de l'analyse des politiques

Tous les utilisateurs d'espace de travail peuvent afficher les journaux d'activités associés aux modifications apportées dans la page d'analyse des politiques dans l'historique de l'espace de travail (voir Journaux d'activités et historique des versions).

- Activer l'analyse des politiques

Figure 312: Activer l'analyse des politiques

- Désactiver l'analyse des politiques

Figure 313: Désactiver l'analyse des politiques

- Mettre à jour l'analyse des politiques

Figure 314: Mettre à jour l'analyse des politiques

Appliquer des politiques

Cisco Secure Workload peut appliquer des politiques en utilisant :

- Déployer des agents logiciels sur les charges de travail, on page 19 installés sur les charges de travail individuelles :
  - Linux
  - Windows
  - Kubernetes/OpenShift

  Pour les détails techniques sur le fonctionnement des agents sur chaque plateforme, consultez les Application des politiques par le biais d'agents, on page 55 et Application des conteneurs, on page 566.
- Connecteurs infonuagiques
  - AWS par l'intermédiaire de Connecteur AWS, on page 241
  - Azure par l'intermédiaire de Connecteur Azure, on page 256
- Intégrer les équilibreurs de charge par l'intermédiaire d'un orchestrateur externe :
  - F5 BIG-IP, on page 159
  - Citrix Netscaler, on page 166
- Intégration avec Cisco Secure Firewall Management Center, on page 347
- Diffusion en flux continu vers des orchestrateurs tiers pour mise en application dans une infrastructure tierce

Caution Lorsque vous appliquez des politiques, le système insère de nouvelles règles de pare-feu sur les hôtes concernés et supprime toutes les règles existantes sur ces derniers.

Vérifier l'intégrité de l'agent et la préparation à la mise en application

Certaines de ces vérifications peuvent être effectuées avant ou après l'application de la politique.

Des autorisations peuvent être nécessaires pour modifier les capacités de l'agent ou du connecteur; Consultez les exigences et les prérequis dans les chapitres pertinents.

Vous n'avez pas besoin d'effectuer ces vérifications pour les charges de travail pour lesquelles vous n'avez pas l'intention d'appliquer des politiques.

Vérifiez que :	Autres renseignements
Les agents sont installés sur toutes les charges de travail de la portée qui sont associées à l'espace de travail objet de la mise en application	Cliquez sur **Defend (défense) » Segmentation (défense)** et accédez à la portée et à l'espace de travail appropriés. Cliquez sur **Matching Inventories** (Correspondance des inventaires), puis sur **IP Addresses** (Adresses IP). Les adresses IP sous cet onglet ne comportent généralement pas d'agents installés, et les agents doivent généralement être installés pour appliquer la politique. Exceptions : l'application a lieu pour les types d'inventaire suivants qui s'affichent dans l'onglet IP Addresses (adresses IP) : • Inventaire infonuagique sur lequel la politique est appliquée à l'aide d'un connecteur infonuagique. (L'installation des agents sur les charges de travail individuelles est facultative). • Les adresses Kubernetes apparaissent dans la liste des adresses IP si les agents sont installés sur des pods de charge de travail individuels; L'inventaire de Kubernetes avec les agents installés s'affiche sous l'onglet « Pods ».
La version de l'agent installé est à jour et prise en charge	Pour obtenir un aperçu des versions des agents installées, cliquez sur **Manage (Gérer) > Agents (agents)**, puis cliquez sur **Distribution** (diffusion) et consultez le tableau **Distribution Version Software Agent** (distribution des versions des logiciels de l'agent). Pour en savoir plus, cliquez sur **Manage (Gestion) > Agents (Agents)** , puis sur **Agents List (Liste des agents)** .
Les agents installés ont une capacité d'application.	Cliquez sur **Manage (Gestion) > Agents (Agents)**, puis sur **Convert to Enforcement Agent(Conversion en agent d'application)**. Dans la zone **Filter** (filtre), saisissez **`Agent Type = Advanced Visibility (visibilité approfondie).`** Convertir tous les agents qui doivent appliquer la politique.
L'application est activée pour tous les agents.	(Cette exigence est distincte de l'assurance que les agents ont des capacités d'application et de l'activation de l'application dans l'espace de travail). **Important!** Selon votre déploiement, cela peut être fait avant ou après avoir mis en application l'espace de travail. Vérifiez que Vérifier l'application est activée pour les agents.
L'application est activée pour les mécanismes d'application autres que d'agent	**Important!** N'activez pas la mise en application sur les connecteurs infonuagiques sans agents TANT QUE VOUS N'AVEZ PAS mis en application la politique sur l'espace de travail. Les orchestrateurs externes qui prennent en charge l'application doivent également être activés avant de pouvoir être appliqués.

Vérifiez que :	Autres renseignements
Le paramètre **Preserve Rules** (Conserver les règles) du profil de configuration de l'agent est approprié pour la plateforme de charge de travail	• Pour Kubernetes/OpenShft, consultez la section relative à l'application sur les conteneurs. • Pour les autres plateformes, consultez les informations pour chaque plateforme dans la section Agents logiciels. Conseil : Recherchez « Conserver les règles » dans ce document pour trouver des informations utiles.
(Une fois l'espace de travail appliqué). Tous les agents ont reçu les politiques applicables à la charge de travail	Consultez la section Vérifier si les politiques appliquées sont envoyées aux agents.
Les agents sont intègres	En plus des sources ci-dessus, les emplacements suivants contiennent des informations sur l'intégrité des agents : • Cliquez sur **Manage > Agents (Gestion > Agents)**, puis sur **Monitor**(surveillance). Regardez les informations sous **Enforcement Agents** Agents d'application). • Cliquez sur **Manage > Agents (Gestion > Agents)**, puis sur **Distribution**. Choisissez le type d'agent dans le haut de la page. • Cliquez sur le filtre **Organize > Scopes and Inventory (Organiser> Portées et inventaire)**, pour trouver une charge de travail spécifique d'intérêt, puis cliquez sur l'adresse IP. La page **Workload Profile** (Profil de la charge de travail) s'ouvre dans une fenêtre de navigateur distincte comprenant un panneau Intégrité de l'agent. Pour en savoir plus, consultez la section Profil de charge de travail.

Activer l'application des politiques

Caution L'application des politiques supprime les règles de pare-feu existantes et écrit de nouvelles règles de pare-feu pour chaque charge de travail de la portée qui est affectée par cet espace de travail.

Si vous n'avez pas totalement vérifié que vos politiques fonctionnent correctement, leur mise en application peut modifier le fonctionnement de vos applications et perturber les tâches opérationnelles.

Before you begin

- Pour commencer, lorsque vous appliquez des politiques, envisagez de définir la règle collectrice sur Allow (autoriser). Ensuite, surveillez le trafic pour voir ce qui correspond à la règle collectrice.

Lorsqu'aucun trafic nécessaire ne correspond à la règle « collectrice », vous pouvez définir ce paramètre sur Deny (Refuser).

- Si vous appliquez des espaces de travail dans plusieurs portées à la fois, vous ne pouvez appliquer que les espaces de travail analysés. Si vous appliquez un espace de travail unique en utilisant la deuxième méthode décrite dans la procédure ci-dessous, l'analyse des politiques de l'espace de travail avant de l'appliquer est recommandée, mais est non obligatoire.

  Consultez la section Analyse des politiques en temps réel et sous-sections.

- L'assistant pour l'application d'une seule portée est plus détaillé que celui qui offre la possibilité d'appliquer plusieurs portées simultanément. Si vous avez besoin des fonctionnalités de Assistant d'application des politiques, on page 564, utilisez la deuxième méthode décrite dans la procédure ci-dessous.

- **IMPORTANT!** Vérifiez que les politiques sont correctes.

  Les résultats des politiques dans n'importe quel espace de travail peuvent être affectés par les politiques appliquées dans d'autres portées. Avant que l'application des politiques ne soit activée sur un espace de travail, la page Policy Enforcement (Application des politiques) montre comment les flux sont touchés par les politiques appliquées dans les espaces de travail associés à d'autres portées. Par exemple, une politique générale « Les hôtes de production ne doivent pas communiquer avec les hôtes hors production » de l'espace de travail appliqué d'une portée parente peut avoir une incidence sur le trafic sur les charges de travail appartenant à une application dans une portée enfant.

  Si aucun nouveau renseignement ne s'affiche dans les tableaux Enforcement (d'application), assurez-vous que la bonne plage temporelle est sélectionnée.

  Pour en savoir plus sur les informations que vous voyez sur la page Enforcement (Application), consultez Analyse des politiques en temps réel et sous-sections. (Les mêmes renseignements concernant l'analyse en direct s'appliquent également à la page Application de la politique).

  Si les résultats de l'analyse en direct diffèrent des résultats sur la page Enforcement (d'application), assurez-vous que les portées, les versions de politiques et la plage temporelle analysées sont les mêmes que les portées, les versions de politiques et la plage temporelle utilisés pour générer des résultats sur la page d'application.

- Découvrez comment les agents appliquent les politiques sur chaque plateforme. Consultez :
  - Pour les charges de travail Windows et Linux, consultez les Application des politiques par le biais d'agents, on page 55 et les rubriques secondaires.
  - Pour Kubernetes et OpenShift, consultez

    Application des conteneurs, on page 566.
  - Pour les équilibreurs de charge, consultez

    Application de la politique pour Citrix Netscaler, on page 168 et

    Application de la politique pour F5 BIG-IP, on page 162.
  - Pour les charges de travail infonuagique configurées à l'aide de connecteurs infonuagiques, consultez :
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, on page 252 et les rubriques connexes.
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, on page 263 et les rubriques connexes.

- Vous devez avoir les autorisations requises pour appliquer des politiques :

  Vous devez avoir la capacité Appliquer ou supérieure sur la portée. Les utilisateurs disposant d'autres capacités sur la portée peuvent toujours afficher cette page, mais ne pourront pas appliquer (ou désactiver) les nouvelles politiques.

- Vérifiez que tous les agents installés pertinents et les autres points terminaux d'application, tels que les connecteurs infonuagiques, sont prêts à appliquer la politique. Pour obtenir la liste des vérifications de l'intégrité et de la préparation des agents, consultez Vérifier l'intégrité de l'agent et la préparation à la mise en application, on page 558.

Note Certaines de ces vérifications doivent être effectuées après la mise en application; par exemple, vous ne devez activer l'application sur les connecteurs infonuagiques qu'après avoir activé l'application dans l'espace de travail. Pour les agents installés, vous activez généralement l'application dans la configuration de l'agent avant d'appliquer l'espace de travail.

Procedure

Étape 1 Dans le volet de navigation, choisissez **Defend** > **Segmentation**(défendre la segmentation).

Étape 2 Vous pouvez appliquer des politiques pour une ou plusieurs portées à la fois :

Pour appliquer la politique à plusieurs portées à la fois :

(Seuls les espaces de travail qui ont été analysés peuvent être appliqués à l'aide de ce processus).

a) Cliquez sur le signe d'insertion sur le côté droit de la page pour afficher le volet Tools (outils) :
b) Cliquez sur **Enable Enforcement** (Activer l'application).
c) Cliquez sur **Next** (suivant) pour démarrer l'assistant.
d) Sélectionnez un espace de travail à mettre en application.

   (L'option permettant l'application d'espaces de travail pour des portées supplémentaires se trouve sur la dernière page de l'assistant).

e) Cliquez sur **Next** (suivant).
f) Choisissez la version de cet espace de travail à appliquer, puis cliquez sur **Next** (Suivant).
g) Pour appliquer simultanément les politiques à une autre portée, cliquez sur **+ Add Another Workspace** (+ Ajouter un autre espace de travail) et procédez comme suit.

   Répétez l'opération si nécessaire pour les autres portées.

h) Cliquez sur **Accept and Enforce** (Accepter et appliquer).

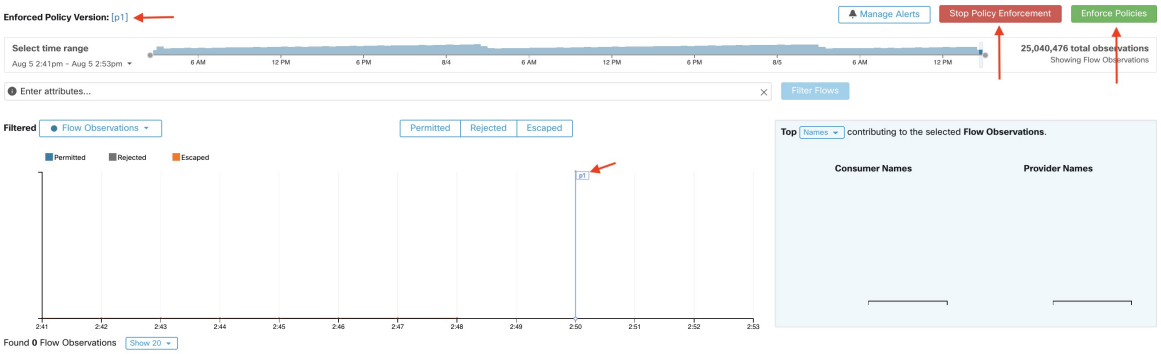
Pour appliquer des politiques à une seule portée :

a) Accédez à l'espace de travail principal de la portée pour laquelle vous souhaitez appliquer la politique.
b) Cliquez sur **Manage Policies** (Gestion des politiques).
c) Cliquez sur **Enforcement** (Mise en application).
d) Cliquez sur **Enforce Policies** (Appliquer les politiques).
e) Suivez les étapes de l'assistant.

   Pour en savoir plus sur l'assistant, consultez Assistant d'application des politiques, on page 564.

Étape 3 Cliquez sur **Accept and Enforce** (Accepter et appliquer) sur la dernière page de l'assistant pour envoyer les nouvelles règles de pare-feu vers les ressources concernées par les politiques dans cet espace de travail. Un indicateur d'étiquette est créé au moment de l'application :

Figure 315: Page Policy Enforcement (Application de la politique) avec Mise en application activée



Vous devrez peut-être actualiser la page pour voir l'indicateur.

What to do next

- Si vous avez appliqué une politique pour un seul espace de travail, demandez-vous si l'application de la politique doit également concerner d'autres espaces de travail d'autres portées afin d'obtenir les résultats escomptés en matière d'application.

  Par exemple, il peut être nécessaire d'appliquer la politique aux espaces de travail pour les portées ascendantes ou les portées qui incluent des charges de travail impliquées dans des politiques inter-portées.

- L'application n'aura pas lieu tant que la mise en application n'est pas activée pour les agents, les connecteurs infonuagiques ou les orchestrateurs externes qui assurent l'application des politiques :
  - Pour les charges de travail sur lesquelles des agents sont installés, appliquez la politique dans la configuration de l'agent pour les portées et les filtres d'inventaire pertinents. Consultez Configuration de l'agent logiciel, on page 80 et les sous-sections.
  - Pour les charges de travail infonuagique configurées à l'aide de connecteurs infonuagiques, consultez :
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, on page 252 et les rubriques connexes.
    - Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, on page 263 et les rubriques connexes.
  - Pour Kubernetes et OpenShift consultez :
    - Application des conteneurs, on page 566
    - Configuration de l'agent logiciel, on page 80
  - Pour les équilibreurs de charge, consultez :
    - Application de la politique pour F5 BIG-IP, on page 162

      Application des politiques au contrôleur d'entrée F5, on page 163

• Application de la politique pour Citrix Netscaler, on page 168

- Vérifiez que la mise en application fonctionne comme prévu. Consultez Vérifier que l’application fonctionne comme prévu, on page 567.
- Configurez les alertes pour être informé de tout problème, par exemple si les flux sont rejetés après l’activation de la mise en application.

Assistant d'application des politiques

Lorsque vous appliquez des politiques pour un seul espace de travail à partir de la page d’application de l’espace de travail, l’assistant d’application de politiques vous permet de :

- Passer en revue les politiques avant de les mettre en œuvre sur les charges de travail.

  Cela inclut les politiques héritées des portées ascendantes.
- Télécharger les modifications à la politique pour examen.
- Comparer les versions.
- Choisissez la version analysée de l’espace de travail à appliquer.
- Restaurer les politiques à une version précédente.

Étapes de l’assistant d’application des politiques :

1. Sélectionnez les mises à jour des politiques

   Vous pouvez sélectionner la version des politiques à appliquer aux charges de travail.

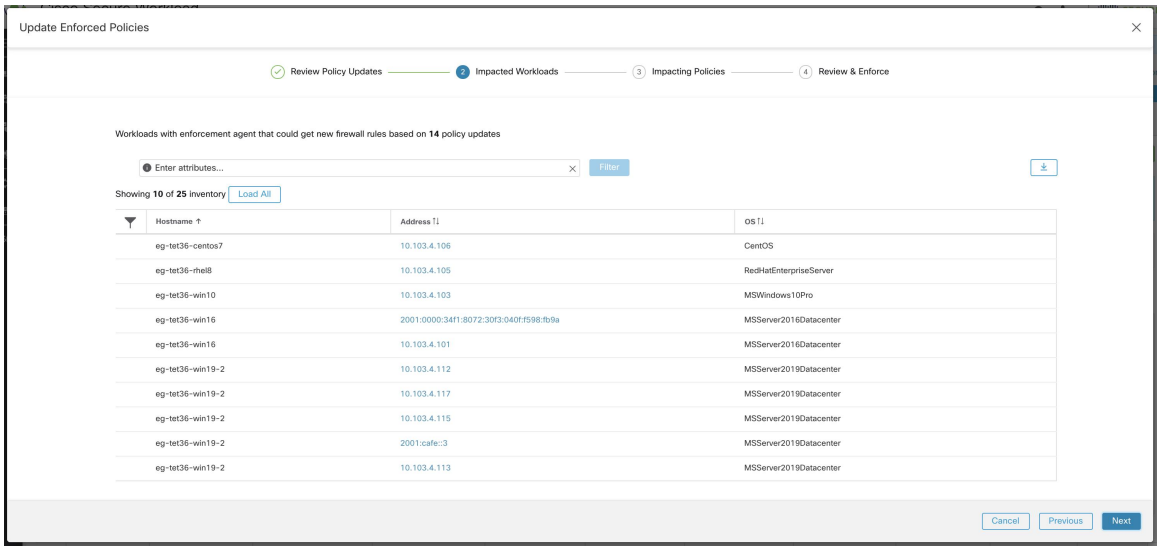
   La différence entre les politiques actuellement appliquées et les politiques dans la version sélectionnée s’affiche.

   De même pour Comparaison des versions des politiques : différence de politique ((Différences des politiques), vous pouvez filtrer et examiner les modifications de politique et les télécharger au format CSV.
2. Charges de travail affectées

   Cette étape affiche les charges de travail qui seront affectées par les nouvelles règles de pare-feu générées à partir des modifications de politique sélectionnées. Le résultat provient de la recherche de toutes les charges de travail qui ont des agents d'application dans le groupe des consommateurs/fournisseurs des changements de politique sélectionnés.

   Le nombre de charges de travail potentiellement touchées ne peut pas dépasser le nombre total de charges de travail de la portée. Cependant, le nombre réel de charges de travail concernées peut être plus faible en raison d’autres facteurs tels que les intents de configuration de l’agent.

Figure 316: Liste des charges de travail affectées

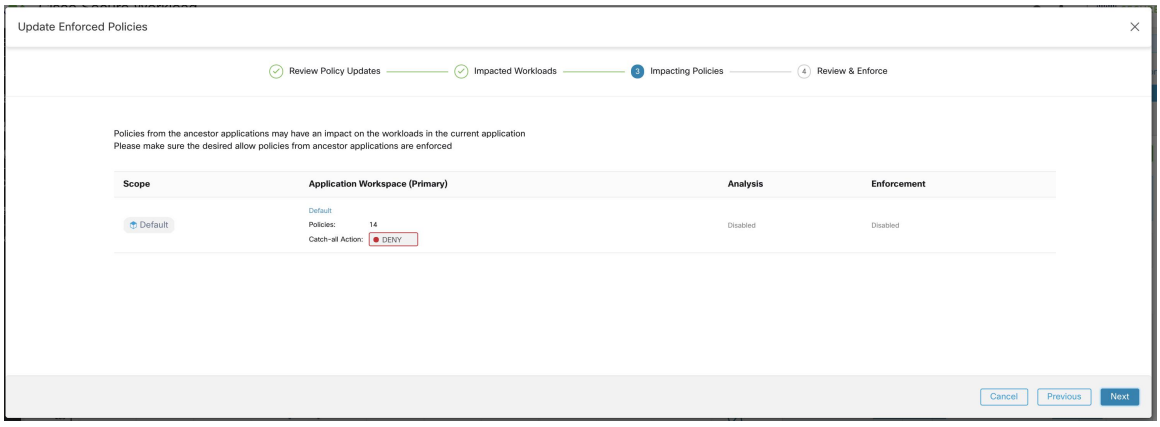


Pour plus de détails sur l'affichage, le filtrage et le téléchargement des éléments de l'inventaire, consultez Inventory, on page 349.

3. Politiques ayant une incidence

   Les politiques des espaces de travail ascendants peuvent avoir une incidence sur les charges de travail de l'espace de travail actuel. Par conséquent, vous devez vous assurer que les politiques d'autorisation souhaitées des espaces de travail ascendants sont appliquées.

   Figure 317: Liste des espaces de travail ascendants et des versions appliquées

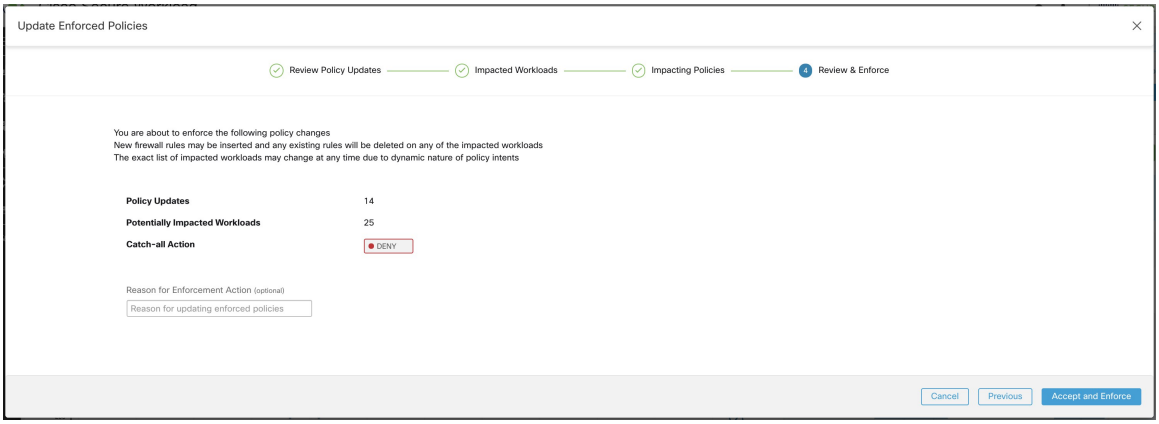


4. Lire attentivement et accepter.

   Cette dernière étape résume les modifications de politique à appliquer, le nombre de charges de travail potentiellement touchées et l'action globale qui sera appliquée. Lorsque vous cliquez sur **Accepter et appliquer**, les politiques de l'espace de travail sont utilisées pour calculer les nouvelles règles de pare-feu qui seront configurées sur les charges de travail pertinentes.

   Vous avez la possibilité de fournir un nom, une description et un motif d'action pour les politiques nouvellement appliquées pour référence future. En cas de restauration, vous pouvez fournir uniquement la raison, car le nom et la description d'une version antérieure ne peuvent pas être modifiés.

Figure 318: Examiner le résumé et appliquer les modifications à la politique



Application des conteneurs

Pour obtenir une présentation des étapes requises pour configurer la segmentation sur les charges de travail basées sur des conteneurs qui sont gérées par Kubernetes et OpenShift, consultez Set Up Microsegmentation for Kubernetes-Based Workloads, on page 7.

Attention **Les agents s'exécutant sur des hôtes Kubernetes/OpenShift doivent être configurés pour conserver les règles existantes.**

Afin d'éviter que l'application n'interfère avec les règles iptables ajoutées par Kubernetes, l'agent doit être configuré avec un profil pour lequel l'option **Preserve Rules** (Conserver les règles) est activée. Voir Creating an Agent Config Profile.

Lors de l'application des politiques sur les conteneurs, Cisco Secure Workload permet d'utiliser les abstractions de service Kubernetes/OpenShift en tant que fournisseurs. En interne, les politiques relatives aux abstractions de services sont transformées en règles pour les pods fournisseurs et les nœuds sur lesquels ils s'exécutent. Cette transformation dépend du type du service Kubernetes/OpenShift, et elle est mise à jour de manière dynamique chaque fois que des modifications sont reçues du serveur d'API.

L'exemple suivant illustre la souplesse rendue possible par cette fonctionnalité. Tenez compte de la politique suivante, qui autorise le trafic de tous les hôtes et des pods avec l'étiquette *environment = production* vers un service Kubernetes de type *NodePort* avec le nom *db* qui expose le port TCP 27017 sur un ensemble de pods.

Consommateurs	Fournisseur	Protocole/Port	Action
environment = production OU orchestrator_environment = production	orchestrator_system/service_name = db	TCP 27017	Autoriser

Cette politique produira les règles de pare-feu suivantes :

- Sur les hôtes et les pods étiquetés avec *environment = production*, autorisez les connexions sortantes vers tous les nœuds Kubernetes de la grappe à laquelle le service appartient. Cette règle utilise le port de nœud affecté à ce service par Kubernetes.
- Sur les pods avec l'étiquette *environment = production*, autorisez les connexions sortantes vers la ClusterIP attribuée à ce service par Kubernetes. Cette règle utilise le port accessible par le service (TCP 27017).
- Sur les nœuds Kubernetes de la grappe à laquelle le service appartient, autorisez les connexions sortantes vers les pods du fournisseur. Cette règle utilise le port cible accessible par le service (TCP 27017).
- Sur les pods fournissant la base de données de service, autorisez toutes les connexions entrantes de tous les nœuds Kubernetes et des hôtes et pods des consommateurs. Cette règle utilise le port cible accessible par le service (TCP 27017).

Les modifications apportées au type de service, aux ports et à l'ensemble de pods des fournisseurs sont immédiatement détectées par le générateur de règles Cisco Secure Workload et utilisées pour mettre à jour les règles de pare-feu générées.

Caution **Les politiques comprenant l'inventaire Kubernetes/OpenShift doivent être conçues avec soin pour éviter tout conflit avec le fonctionnement interne de la grappe Kubernetes.**

Les éléments Kubernetes/OpenShift importés par Cisco Secure Workload comprennent les pods et les services constituant la grappe Kubernetes (par exemple, les pods dans l'espace de noms du système Kubernetes). Cela permet de définir des politiques précises pour sécuriser la grappe Kubernetes elle-même, mais cela signifie également que des politiques mal conçues peuvent affecter le fonctionnement de la grappe.

Vérifier que l'application fonctionne comme prévu

Vérifier les agents

Consultez Vérifier l'intégrité de l'agent et la préparation à la mise en application, à la page 558.

Vérifier les flux échappés et rejetés

Dans le menu sur le côté gauche de l'écran, cliquez sur **Overview** (Aperçu).

Sur la page **Security Dashboard** (Tableau de bord de sécurité), examinez la **note de conformité de la segmentation**.

Si elle est inférieure à 100, il se peut que vous ayez des flux échappés ou rejetés, ce qui indique un problème de configuration de la politique.

Pour de plus amples renseignements, consultez la section Note de conformité de la segmentation, à la page 858.

Pour plus d'informations sur l'examen de ces situations, consultez Résultats de l'analyse des politiques : comprendre les bases, à la page 548 et les rubriques secondaires. (Les informations dans ces rubriques s'appliquent aux politiques appliquées affichées sous l'onglet Enforcement (Application) et aux politiques analysées affichées sous l'onglet Policy Analysis (Analyse des politiques).)

Ajoutez toutes les politiques manquantes ou modifiez les politiques existantes, par exemple en ajoutant des protocoles ou des ports supplémentaires, pour autoriser le trafic légitime requis.

Effectuez ensuite une nouvelle analyse avant de recommencer l'application de la politique.

Afficher les politiques appliquées pour une charge de travail spécifique (politiques concrètes)

Cette procédure permet d'afficher toutes les politiques appliquées pour une charge de travail spécifique (c'est-à-dire les *politiques concrètes* pour cette charge de travail). Cet affichage est utile, car toutes les politiques d'un espace de travail peuvent ne pas s'appliquer à toutes les charges de travail de ce dernier, et les politiques de plusieurs espaces de travail peuvent s'appliquer à une charge de travail particulière (par exemple, les politiques héritées dans les portées parentes ou encore précédentes).

Les politiques concrètes sont répertoriées par ordre de priorité. Pour en savoir plus sur les effets de la priorité, consultez la section sur les priorités de politique.

Avant de commencer

Remarque Les politiques concrètes ne comprennent que les politiques des espaces de travail ayant fait l'objet de mise en application. Si un espace de travail n'a pas été mis en application, les politiques qui s'appliqueraient à la charge de travail si l'espace de travail était mis en application ne s'affichent pas dans la liste.

Procédure

Étape 1 Vous pouvez accéder à la page des politiques concrètes pour une charge de travail à partir de la page Inventory (Inventaire) ou de l'espace de travail :

Pour accéder à partir de la page Scope and Inventory (Portée et inventaire) :

a) Choisissez **Organize > Scopes and Inventory** (Organiser > Portée et inventaire).
b) Recherchez l'adresse IP de la charge de travail qui vous intéresse et cliquez dessus.

Le profil de charge de travail s'ouvre dans un onglet distinct.

En général, sauf pour les charges de travail infonuagique qui sont gérées sans agents, Kubernetes et les charges de travail OpenShift, si l'adresse IP apparaît dans l'onglet **IP Addresses** (adresses IP) et non dans l'onglet **Workloads** (Charges de travail), cela signifie qu'un agent n'est pas installé sur la charge de travail, Les politiques ne peuvent donc pas être appliquées et il n'y a pas de liste de politiques concrètes.

Pour accéder à partir de la page de segmentation :

a) Choisissez **Defend (défense) > Segmentation (segmentation).**
b) Cliquez sur la portée.
c) Cliquez sur l'espace de travail principal.
d) Cliquez sur **Manage Policies** (Gestion des politiques).
e) Cliquez sur l'onglet **Matching Inventories** (Inventaires correspondants).
f) Recherchez l'adresse IP de la charge de travail qui vous intéresse et cliquez dessus.
g) Dans le panneau qui s'ouvre sur la droite, cliquez sur **View Workload Profile**(afficher le profil de charge de travail).

Le profil de charge de travail s'ouvre dans un onglet distinct.

Étape 2 Dans le menu de gauche de la page du profil de charge de travail, cliquez sur **CONCRETE POLICIES (POLITIQUES CONCRÈTES).**

Étape 3 Cliquez sur une ligne pour afficher les détails.

Pour en savoir plus, consultez l'onglet Politiques concrètes.

Étape 4 Pour voir le volume de trafic qui a atteint chaque politique :

a) Cliquez sur **Get All Stats** (récupérer toutes les statistiques).

b) Cliquez sur chaque politique qui vous intéresse.

Étape 5 Pour afficher des informations sur les charges de travail de Kubernetes ou d'OpenShift cliquez sur **CONTAINER POLICIES** (POLITIQUES DE CONTENEUR).

Prochaine étape

Choisissez **Monitor > Enforcement Status** (Surveiller > État de l'application) pour connaître l'état de politiques concrètes, par exemple pour voir si des politiques ont été ignorées. Pour en savoir plus, consultez la section État de l'application.

Vérifier que la mise en application est activée pour les agents

Procédure

Étape 1 Cliquez sur **Defend > Enforcement Status** (Défendre > État d'application).

Étape 2 Pour afficher uniquement l'état d'application pour une portée spécifique, activez le contrôle **Filter by Scope** (Filtrer par portée) et sélectionnez une portée.

Étape 3 Consultez le tableau **Agent Enforcement Enabled** (Mise en application des agents activée).

Si le tableau indique que des agents sont **Not Enforced** (ne sont pas mis en application), poursuivez cette procédure.

Sinon, ignorez le reste de la procédure, car tous les agents sont activés pour application.

Étape 4 Cliquez sur la section orangée **Not Enforced** (Non appliqué) du tableau pour afficher les charges de travail concernées au sein de la table sous le tableau.

Étape 5 Activez l'application sur ces charges de travail en modifiant le profil de configuration de l'agent.

Consultez Creating an Agent Config Profile, à la page 83.

Vérifier que les politiques appliquées sont transmises aux agents

Pour que l'application ait lieu, les politiques spécifiques à chaque charge de travail doivent être transmises avec succès vers l'agent installé sur cette charge de travail. L'état est également affiché pour l'application des politiques gérée par les connecteurs infonuagiques, même si des agents ne sont pas installés.

Avant de commencer

Appliquer des politiques pour au moins une portée.

Procédure

Étape 1 Cliquez sur **Defend > Enforcement Status** (Défendre > État d'application).

Étape 2 Pour afficher uniquement l'état d'application pour une portée spécifique, activez le contrôle **Filter by Scope** (Filtrer par portée) et sélectionnez une portée.

Étape 3 Consultez le tableau des **politiques concrètes des agents**.

Si le tableau indique que des fichiers sont **ignorés**, poursuivez cette procédure.

Sinon, ignorez le reste de cette procédure.

Étape 4 Pour afficher la liste des charges de travail touchées par ce problème, cliquez sur la partie rouge **Skipped** (Ignoré) du tableau.

Les charges de travail concernées sont répertoriées dans le tableau sous les graphiques.

Étape 5 Pour voir les raisons de ce problème :

Pour chaque charge de travail dans les résultats de la recherche, cliquez sur le bouton **(i)** à côté de **Skipped** (Ignoré) dans la colonne **Concrete Policies** (Politiques concrètes).

Message d'erreur	Autres renseignements
L'agent n'a pas de système d'exploitation Windows	Au moins une politique applicable uniquement aux charges de travail Windows comprend les consommateurs ou les fournisseurs qui n'exécutent pas le système d'exploitation Windows. Supprimez ces charges de travail de ces politiques.
Le nombre maximal de politiques a été atteint	Consultez Si l'agent dispose d'un trop grand nombre de politiques, à la page 570.

Prochaine étape

(Facultatif) Configurez une alerte pour être averti si cette situation se reproduit. Consultez Configurer les alertes, à la page 673.

Si l'agent dispose d'un trop grand nombre de politiques

Si l'ensemble complet des politiques concrètes applicables ne peut pas être transmis à un agent en particulier, la dernière version des politiques n'est pas transmise.

Arrière-plan : Il y a une limite au nombre de politiques prises en charge sur chaque agent. Les limites s'appliquent également aux politiques appliquées à l'aide de connecteurs infonuagiques. Vous trouverez peut-être les renseignements de Limites de configuration dans Cisco Secure Workload, à la page 1167 utiles.

Avant de commencer

Utilisez cette procédure pour résoudre ce problème si Vérifier que les politiques appliquées sont transmises aux agents, à la page 569 indique que l'agent ne peut pas prendre en charge l'ensemble complet des politiques appliquées.

Procédure

Étape 1 Accédez à l'espace de travail principal pour un portée concerné.

Étape 2 Modifiez les politiques dans l'espace de travail principal :

Essayez de réduire le nombre de politiques et de réduire les longues listes d'adresses IP du consommateur ou du fournisseur.

Par exemple, regrouper les politiques existantes et/ou baser les politiques sur les sous-réseaux plutôt que sur de longues listes d'adresses IP.

Pour les politiques appliquées à l'aide d'un connecteur infonuagique, vous pouvez également augmenter les limites imposées par la plateforme. Consultez la documentation de votre plateforme infonuagique.

Étape 3 Après avoir apporté les modifications, utilisez la dernière version de l'espace de travail et vérifiez à nouveau les politiques ignorées.

Étape 4 Répétez cette procédure pour toutes les autres portées rencontrant ce problème.

Modifier les politiques appliquées

Appliquer les politiques nouvelles et révisées

Si vous devez réviser des politiques après leur application, vous effectuez généralement les modifications dans le même espace de travail principal. Ensuite, examinez attentivement vos modifications et analysez à nouveau l'espace de travail pour vous assurer qu'elles produisent l'effet escompté. Lorsque vous êtes certain que les modifications auront l'effet souhaité, cliquez sur le bouton **Enforce Latest Policies**(Appliquer les dernières politiques) dans le coin supérieur droit de la page.

Afficher, comparer et gérer les versions des politiques appliquées

Chaque fois que vous appliquez ou renforcerez des politiques dans un espace de travail après avoir apporté des modifications, une nouvelle version (p*) est créée.

Pour en savoir plus sur la gestion des versions, consultez À propos des versions des politiques (v* et p*), à la page 575.

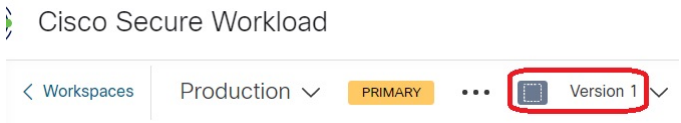
Procédure

Étape 1 Cliquez sur **Defend (Défendre) > Segmentation (Segmentation).**

Étape 2 Accédez au portée et à l'espace de travail principal appropriés.

Étape 3 Cliquez sur **Manage Policies** (Gestion des politiques).

Étape 4 La version actuellement affichée des politiques est indiquée en haut de la page :



La version affichée peut être une version de découverte de politique, une version de politique analysée ou une version de politique appliquée.

Étape 5 Effectuez l'une des opérations suivantes :

Pour afficher une version différente des politiques :	Cliquez sur la version actuelle et choisissez une version différente. Pour obtenir une description des versions, consultez À propos des versions des politiques (v* et p*), à la page 575. **Important!** Si vous choisissez la version av*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 483 au lieu de cette rubrique, sans oublier la mise en garde importante à la fin de celle-ci.
Pour afficher les détails des versions analysées :	1. Cliquez sur **View Version History** (Afficher l'historique des versions) en haut de la page à côté dans la version actuelle. 2. Cliquez sur l'onglet **Published Versions** (Versions publiées) pour voir les versions des politiques analysées et appliquées. 3. Pour afficher les entrées de journal pour une version, cliquez sur le lien dans la version. Les lignes vert clair représentent l'activité d'analyse. Les lignes vert clair représentent l'activité d'application de la politique.
Pour comparer deux versions et voir ce qui a changé :	1. Cliquez sur **Compare Revisions** (Comparer les révisions). 2. Choisissez les versions à comparer. Vous pouvez comparer la dernière version provisoire, les versions analysées et appliquées. 3. Pour en savoir plus sur les résultats, consultez Comparaison des versions des politiques : différence de politique, à la page 577.
Pour supprimer une version indésirable :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Delete** (Supprimer). Les versions de politique publiées (versions p*) peuvent être supprimées tant que la version n'est pas analysée ou appliquée activement.
Pour exporter une version :	Cliquez sur le bouton ⋮ (Autre) dans la version et choisissez **Export...** (Exporter...).. Consultez aussi Exporter un espace de travail, à la page 487.

Prochaine étape

Lorsque vous avez terminé de travailler avec les versions, remplacez la version en haut de la page de l'espace de travail par la dernière version de politique découverte (v*).

Cela évite la suppression involontaire des versions de politiques découvertes et vous permet de créer manuellement des politiques dans l'espace de travail.

Revenir à une version antérieure des politiques appliquées

Pour restaurer les politiques appliquées vers une version précédente, suivez l'un des processus décrits dans Activer l'application des politiques, à la page 560 et choisissez une version antérieure à appliquer.

Désactiver l'application de la politique

- **Pour désactiver l'application des politiques pour plusieurs portées simultanément** :

  Suivez la procédure pour appliquer la politique dans plusieurs portées simultanément, comme décrit dans Activer l'application des politiques, on page 560. Dans la page Select Version (sélectionner une version) de l'assistant, cliquez sur **Select a version** (sélectionner une version) et choisissez **Disable enforcement**) ((désactiver la mise en application).

- **Pour désactiver l'application des politiques pour une seule portée** :

  Accédez à la page Policy Enforcement (application des politiques) de l'espace de travail principal de la portée et cliquez sur le bouton rouge **Stop Policy Enforcement** (Arrêter l'application des politiques). Cela écrit de nouvelles règles de pare-feu dans les ressources de la portée en fonction des politiques appliquées dans les espaces de travail ascendants. Un indicateur d'étiquette avec un « x » sera créé sur le tableau des séries chronologiques.

Suspendre les mises à jour des politiques

Caution Cette option met en pause les mises à jour de politiques pour TOUTES les charges de travail dans TOUTES les portées.

Cette fonctionnalité nécessite des privilèges d'administrateur de site ou de service d'assistance à la clientèle.

Pour suspendre les mises à jour des règles pour tous les points terminaux d'application dans toutes les portées :

1. Dans le volet de navigation, choisissez **Defend (Défendre)** > **Enforcement (Mise en application)** .
2. Cliquez sur l'état à côté de **Policy Updates** (Mises à jour des politiques) .
3. Lisez et acceptez la mise en garde.

Figure 319: Les règles de pare-feu sont mises à jour en permanence

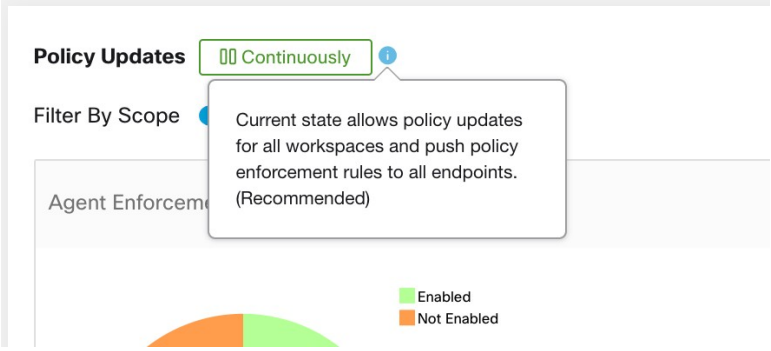


Figure 320: Les mises à jour des règles de pare-feu sont suspendues

Historique de la mise en application

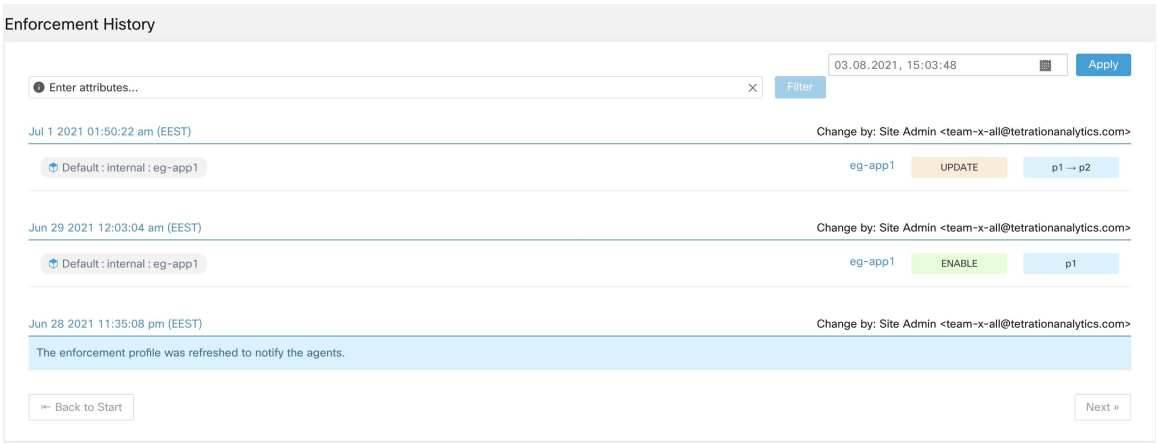
L'historique de mise en application fournit une liste des modifications apportées à la liste des espaces de travail qui ont fait l'objet de l'application de politiques et à leur version.

Pour afficher l'historique de mis en application :

1. Cliquez sur le signe d'insertion sur le côté droit de la page de segmentation pour développer le menu Tools (Outils).
2. Cliquez sur **Enforcement History** (Historique de mise en application).

   Chaque section décrit un événement et affiche un résumé de ce qui a changé.
3. Cliquez sur un événement pour obtenir des renseignements détaillés sur toutes les politiques qui ont été appliquées à ce moment-là.

Figure 321: Affichage de l'historique de mise en application

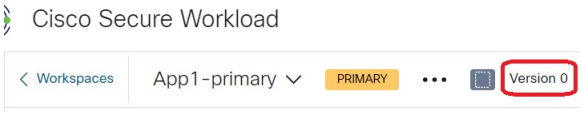


À propos des versions des politiques (v* et p*)

Les versions de politiques sont parfois appelées versions d'espace de travail.

Version affichée

La version des politiques (et des grappes) avec lesquelles vous travaillez actuellement est affichée en haut de la page de l'espace de travail :



- Les versions V* sont générées par la découverte automatique des politiques

  Pour de plus amples renseignements, voir ci-dessous
- Les versions P* sont des versions analysées et/ou appliquées.

  Pour de plus amples renseignements, voir ci-dessous

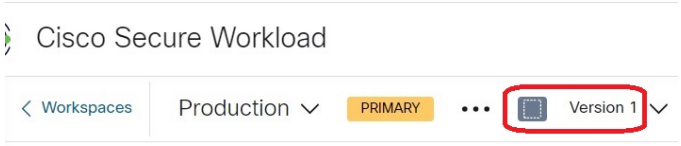
Les icônes suivantes peuvent s'afficher à côté du numéro de version :

Tableau 28 : Icônes de version

	Indique la version des politiques qui est actuellement en cours d'analyse
	Indique la version des politiques actuellement appliquées
	Indique la dernière version des politiques découvertes automatiquement
(sans icône)	Indique que la version n'est pas la dernière version de son type

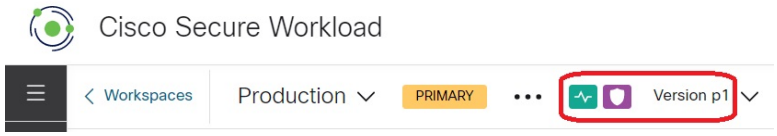
Exemples :

- La version affichée est la dernière version découverte des politiques :



- La version affichée est la version des politiques qui est actuellement en cours d'analyse :

- La version affichée est la version des politiques actuellement en cours d'analyse et d'application :



Version de découverte des politiques (v*)

Chaque fois que vous découvrez automatiquement les politiques pour un espace de travail, la version (v*) est incrémentée.

La première fois que vous découvrez automatiquement les politiques, la version 1 est générée, et toutes les modifications ultérieures à cette exécution, telles que la modification ou l'approbation des grappes (à l'exception d'une réexécution), sont également regroupées sous la version 1. Lorsque vous découvrez ensuite automatiquement les politiques, une nouvelle version est générée (sauf si la découverte échoue).

La version v* est également incrémentée si vous importez des politiques.

Pour utiliser les versions v*, consultez Afficher, comparer et gérer les versions de politiques découvertes, à la page 483.

Version publiée de la politique (p*)

Le terme version de politique « publiée » (p*) pour un espace de travail peut faire référence à :

- La version des politiques qui a été analysée, ou
- La version des politiques qui a été appliquée

Il s'agit de deux versions distinctes mais parallèles qui dépendent du contexte :

- Version de la politique pour l'analyse :

  Chaque fois que vous analysez des politiques dans un espace de travail ou que vous cliquez sur **Analyser les dernières politiques** après avoir apporté une modification, le système prend un instantané de toutes les grappes et toutes les politiques définies dans cet espace de travail, et du numéro de version de politique « publiée » (p*) pour les incréments d'analyse. La dernière version **de l'analyse des politiques en direct** est affichée dans le coin supérieur gauche de la page sur l'onglet Policy Analysis (analyse des politiques) de l'espace de travail principal.

- Version de la politique pour application :

  Chaque fois que vous activez l'application des politiques dans un espace de travail, ou réactivez l'application après avoir apporté des modifications, la version « publiée » des politiques (p*) pour l'application devient le numéro dans la version analysée que vous choisissez dans l'assistant d'application. Ainsi, si vous appliquez la version analysée 5, la version appliquée est également la version 5, même s'il s'agit, par exemple, de la première application de la politique pour l'espace de travail. La **version actuelle de la politique appliquée** est affichée dans le coin supérieur gauche de la page sous l'onglet Enforcement (Application) de l'espace de travail principal.

Gestion des versions publiées (p*)

Les versions de politique publiées ne peuvent pas être modifiées, seulement entièrement supprimées.

Remarque Les versions de politique publiées (p*) sont limitées à 100 au total. Une fois cette limite atteinte, vous devez supprimer des anciennes versions.

Pour gérer et supprimer les versions p*, consultez Afficher, comparer et gérer les versions des politiques analysées, à la page 556ou Afficher, comparer et gérer les versions des politiques appliquées, à la page 571.

Vous pouvez également utiliser l'API pour supprimer des versions publiées.

Comparaison des versions des politiques : différence de politique

Pour comparer les politiques, consultez l'une des rubriques suivantes : Afficher, comparer et gérer les versions de politiques découvertes, on page 483, Afficher, comparer et gérer les versions des politiques analysées, on page 556ou Afficher, comparer et gérer les versions des politiques appliquées, on page 571

Les modifications de politique seront affichées dans trois catégories : Absolute (Absolu), Default (Par défaut) and Catch All (Collectrice). Dans le tableau de comparaison :

- Les différents services appartenant à la même politique sont regroupés
- Filtrer les modifications de politique par facette ou par type de différence
- Les modifications de politique et les services sont paginés

- Télécharger les modifications de politique filtrées au format CSV

Table 29: Propriétés du filtre à facette

Propriété	Description
Priority	P. ex.100
Action	P. ex., ALLOW (AUTORISER), DENY (REFUSER)
Consumer	P. ex. Grappe de consommateurs
Provider	P. ex. Grappe de fournisseurs
Port	P. ex. 80
Protocol	P. ex. TCP

Table 30: Colonnes de sortie CSV

Colonne	Description
Rank	La catégorie de la politique. p. ex., ABSOLUTE (ABSOLUE), DEFAULT (PAR DÉFAUT), CATCH_ALL (COLLECTRICE)
Diff	Le type de différence de la modification. P. ex., ADDED (AJOUTÉ), REMOVED (RETIRÉ), UNCHANGED (NON MODIFIÉ)
Priority	P. ex.100
Action	P. ex., ALLOW (AUTORISER), DENY (REFUSER)
Consumer Name	Le nom de la grappe de consommateurs.
Consumer ID	ID de la grappe de consommateurs.
Provider Name	Nom de la grappe de fournisseurs.
Provider ID	ID de la grappe de fournisseurs.
Protocol	P. ex. TCP
Port	P. ex. 80

Dans la figure ci-dessous, les versions de politique p1 et v1 sont comparées.

Figure 322: Vue des différences des politiques

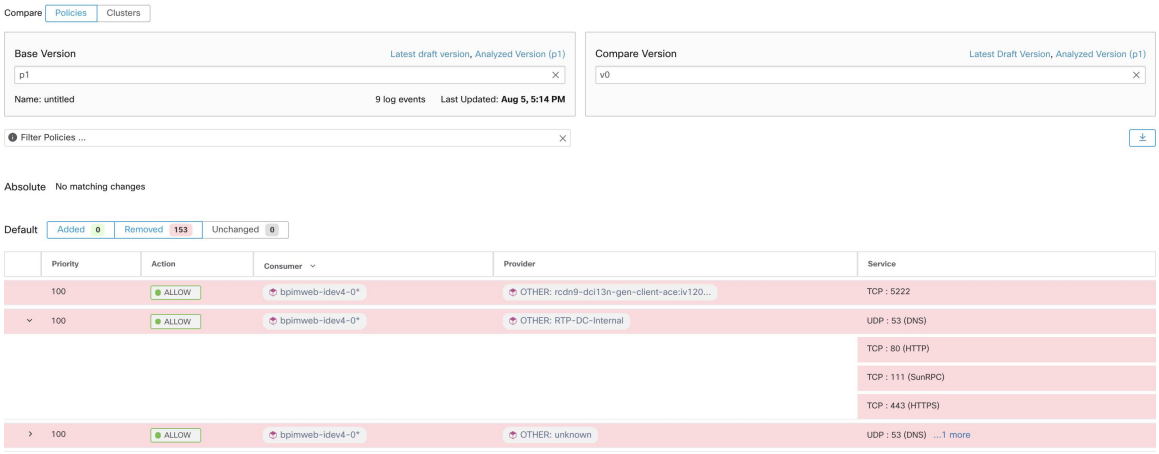


Figure 323: Bouton de téléchargement de l'affichage des différences des politiques

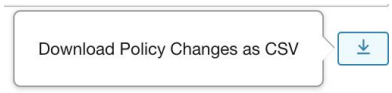


Figure 324: Filtrage de la vue des différences entre les politiques

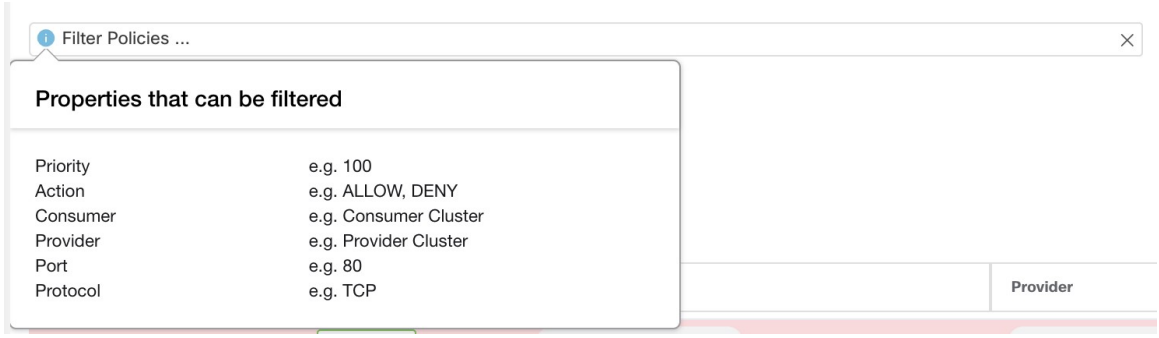


Figure 325: Filtre de type de différence de l'affichage des différences entre les politiques

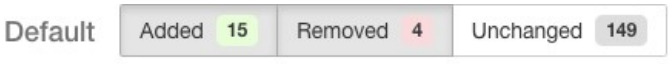


Figure 326: Regroupement des vues des différence entre les politiques

Figure 327: Sortie CSV de l'affichage de la différence entre les politiques

Rank	Diff	Priority	Action	Consumer Name	Consumer ID	Provider Name	Provider ID	Protocol	Port
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	80
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	111
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: RTP-DC-Internal	610bcda7a51e713db909d9fe	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	UDP	53
DEFAULT	ADDED	100	ALLOW	bpimweb-idev4-0*	610bcda7a51e713db909da40	OTHER: unknown	610bcda7a51e713db909da45	TCP	443
DEFAULT	ADDED	100	ALLOW	bpimweb-idev3-0*	610bcda7a51e713db909da26	OTHER: rcdn9-dci13n-gen-client-ace:iv120	610bcda7a51e713db909d9f1	TCP	5222

Tip Consultez aussi Comparaison des versions des grappes générées : vues des différences, on page 511.

Journaux d'activités et historique des versions

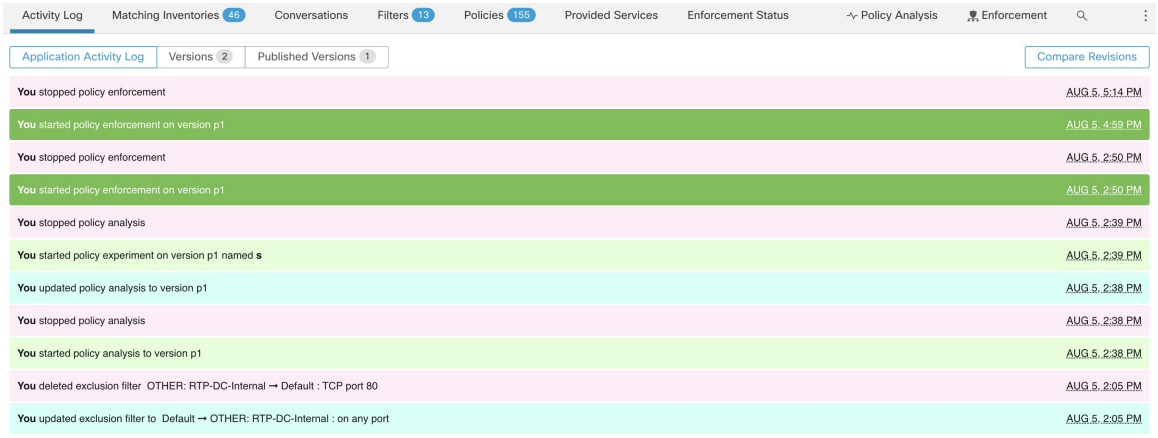
Les journaux d'activités enregistrent l'historique des modifications que vous avez appliquées à un espace de travail. Les événements affichés comprennent l'ajout, la suppression et le changement de nom de charges de travail et de grappes, le déplacement de charges de travail entre les grappes, le chargement de renseignements secondaires, la soumission et l'abandon de la découverte automatique des politiques, etc. La vue montre quel utilisateur a effectué chaque modification.

Pour afficher l'historique des modifications pour un espace de travail, cliquez sur n'importe quel lien du **journal des activités** dans l'espace de travail.

Par exemple :

1. Cliquez sur **Defend (défendre) > Segmentation (segmentation).**
2. Cliquez sur la portée et l'espace de travail appropriés.
3. Cliquez sur le lien **View Activity Log** (Afficher les journaux d'activité).
4. Cliquez sur l'onglet **Workspace Activity Log** (Journal d'activité de l'espace de travail).

Figure 328: Journal des événements applicables à la version v1 de cet espace de travail



Pour en savoir plus sur les onglets et les options de la page relatifs à la version, consultez :

- À propos des versions des politiques (v* et p*), on page 575
- Afficher, comparer et gérer les versions de politiques découvertes, on page 483
- Afficher, comparer et gérer les versions des politiques analysées, on page 556
- Afficher, comparer et gérer les versions des politiques appliquées, on page 571

Suppression automatique des anciennes versions des politiques

Chaque semaine, les éléments suivants sont automatiquement supprimés : les versions d'espace de travail qui n'ont pas été consultées depuis six mois et les politiques de test auxquelles il n'a pas été accédé au cours des 30 derniers jours.

Conversations

Une conversation est définie comme un service fourni par un hôte sur un port particulier et utilisé par un autre hôte. Une telle conversation se matérialise à partir de nombreux flux sur des instants différents. La découverte automatique de politiques prend tous ces flux, ignore les ports éphémères/clients et les dédouble pour générer le graphe de conversation. Pour toute conversation donnée entre l'hôte A et l'hôte B sur le port N du serveur (fournisseur), il y a eu au moins une observation de flux de A à B sur le port N au cours de la période pour laquelle la découverte automatique des politiques a été effectuée.

Utilisez les données de flux pour mieux comprendre quels flux sont associés à quel processus tout en évaluant les grappes générées lors de la découverte automatique des politiques.

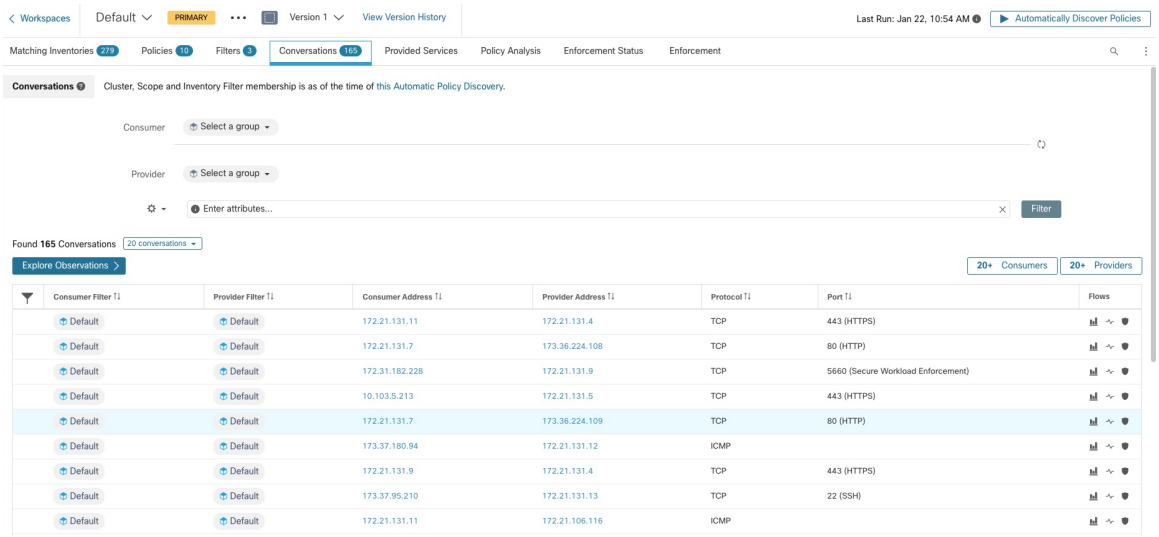
En outre, les informations collectées par les agents offrent une visibilité sur les ports L4 inutilisés. Les ports inutilisés sont ceux pour lesquels aucune communication n'a été constatée pendant l'intervalle sélectionné pour la découverte automatique des politiques. Ces informations peuvent être utilisées pour ouvrir des politiques de communication sur ces ports OU pour fermer les applications se rapportant aux ports inutilisés, réduisant ainsi la surface d'attaque de la charge de travail.

Notez que la classification client-serveur affecte la vue de la conversation de découverte automatique des politiques – elle détermine quel port doit être abandonné (jugé éphémère) dans l'agrégation : consultez Classification client-serveur.

Vue du tableau Conversations

La vue du tableau Conversations offre un moyen simple de visualiser les flux agrégés à partir de la durée de la découverte automatique des politiques, lorsque le port consommateur est supprimé et qu'il n'y a qu'un seul enregistrement pour toute la durée de la recherche. Alors que les politiques vont d'un filtre à l'autre, les conversations vont d'une adresse IP à l'autre.

Figure 329: Vue du tableau Conversations

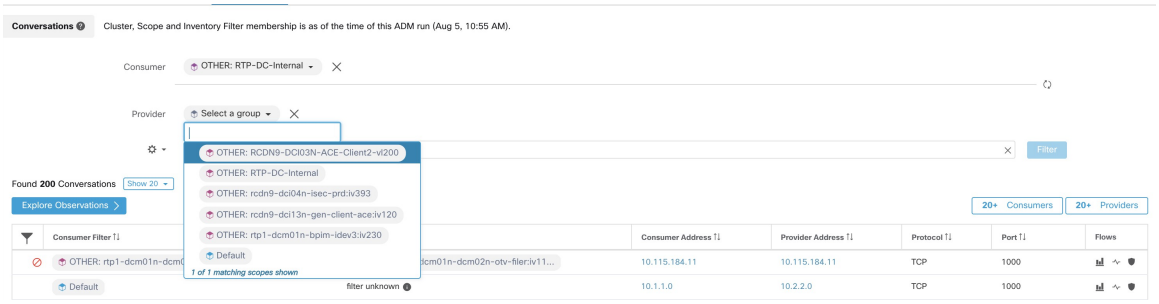


Choix du consommateur ou du fournisseur

Les consommateurs et les fournisseurs peuvent être sélectionnés à l'aide d'un sélecteur déroulant à présélection qui permet de choisir les filtres d'inventaire, les portées et les grappes, comme le montre l'exemple ci-dessous. Toutes les conversations entre le consommateur et le fournisseur choisis sont affichées. Remarque : pour supprimer un filtre existant, cliquez sur l'icône « x » (l'effacement du filtre peut ne pas fonctionner).

Par défaut, le consommateur et le fournisseur correspondent à tous les filtres d'inventaire dont une adresse IP est membre lors de la découverte automatique des politiques. Par exemple, la recherche de la « portée racine » correspondra à toutes les conversations, même si certaines adresses IP pourraient mieux correspondre à des portées plus spécifiques. Pour effectuer une correspondance plus précise, sélectionnez « Restrict scope filtering to an IP's best match (Restreindre le filtrage à l'utilisation d'une adresse IP) » dans la liste déroulante des paramètres à gauche de l'entrée du filtre à aspects.

Figure 330: Choix du consommateur ou du fournisseur



Filtres de conversations

Figure 331: Filtres de conversations

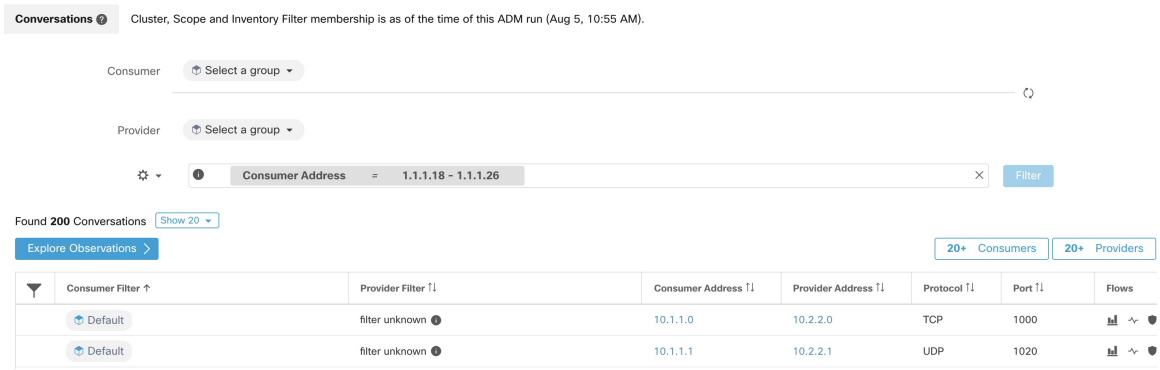
C’est ici que vous définissez les filtres pour affiner les résultats de la recherche. On peut consulter toutes les dimensions possibles en cliquant sur l’icône (?) à côté du mot Filters (Filtres). Pour toutes les données d’étiquettes d’utilisateur, ces colonnes sont également disponibles pour les intervalles appropriés. Cette entrée prend également en charge les mots-clés and, or, not et parenthesis, utilisez-les pour concevoir des filtres plus complexes. Par exemple, un filtre indépendant de la direction entre IP 1.1.1.1 et 2.2.2.2 peut s’écrire :

Adresse du consommateur = 1.1.1.1 et adresse du fournisseur = 2.2.2.2 ou Adresse du consommateur = 2.2.2.2 et adresse du fournisseur = 1.1.1.1. Pour filtrer également sur Protocole = TCP :

(Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1) and Protocol = TCP

L’entrée du filtre prend également en charge les « , » et « - » pour le port, l’adresse du client et l’adresse du fournisseur, en transformant « - » en requêtes de plages. Voici des exemples de filtres valables :

Figure 332: L’entrée du filtre prend en charge la requête de plage pour l’adresse du consommateur



Filtres disponibles :

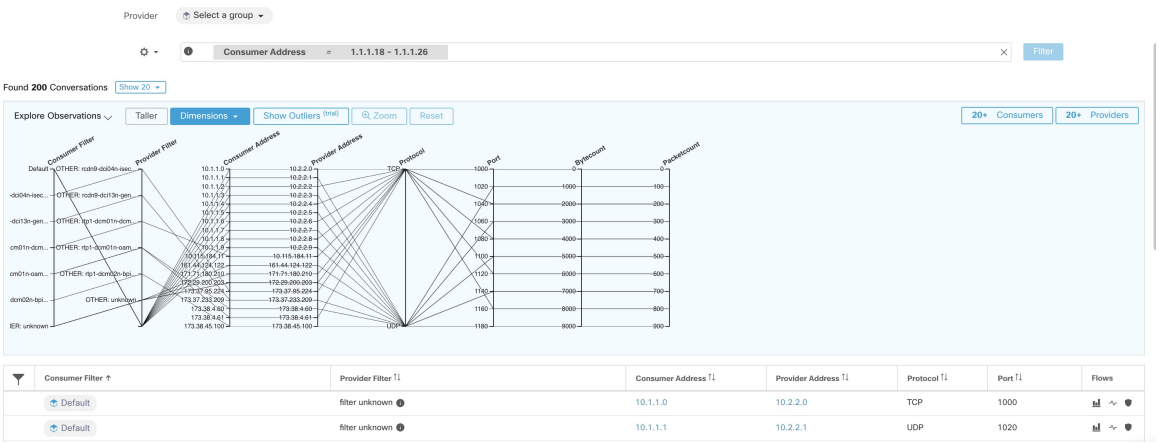
Filtres	Description
Adresse du client	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux observations de flux de conversation dont l’adresse du consommateur chevauche l’adresse IP ou le sous-réseau fourni.
Adresse du fournisseur	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux observations de flux de conversation dont l’adresse du fournisseur chevauche l’adresse IP ou le sous-réseau fourni.
Port	Correspond aux observations de flux de conversation dont le port chevauche le port fourni.
Protocol	Filtrez les observations de flux de conversation par type de protocole (TCP, UDP, ICMP).
Address Type (Type d'adresse)	Filtrez les observations de flux de conversation par type d’adresse (IPv4, IPv6, DHCPv4).

Filtres	Description
Confiance	A indiqué la confiance dans le sens du flux. Valeurs possibles : élevée, très élevée, modérée.
Exclu?	Mettre en correspondance les conversations qui sont exclues par un filtre d'exclusion ou une politique approuvée.
Exclu par	Mettre en correspondance les conversations exclues par un filtre spécifique. Les valeurs possibles : filtre d'exclusion, politique.

Explorer les observations

Cliquer sur le bouton « Explorer les observations » pour activer un affichage graphique qui permet une exploration rapide des données comportant de nombreuses dimensions à l'aide d'un graphique en « coordonnées parallèles ». Un peu impressionnant au premier abord, ce tableau peut être utile pour activer uniquement les dimensions qui vous intéressent (en décochant les éléments du menu déroulant Dimensions) et pour réorganiser l'ordre des dimensions. Une seule ligne dans ce graphique représente une seule observation et l'intersection de cette ligne avec les différents axes indique la valeur de cette observation pour cette dimension. Cela devient plus clair lorsque l'on passe le curseur sur la liste des observations sous le graphique pour voir la ligne en surbrillance représentant l'observation dans le graphique :

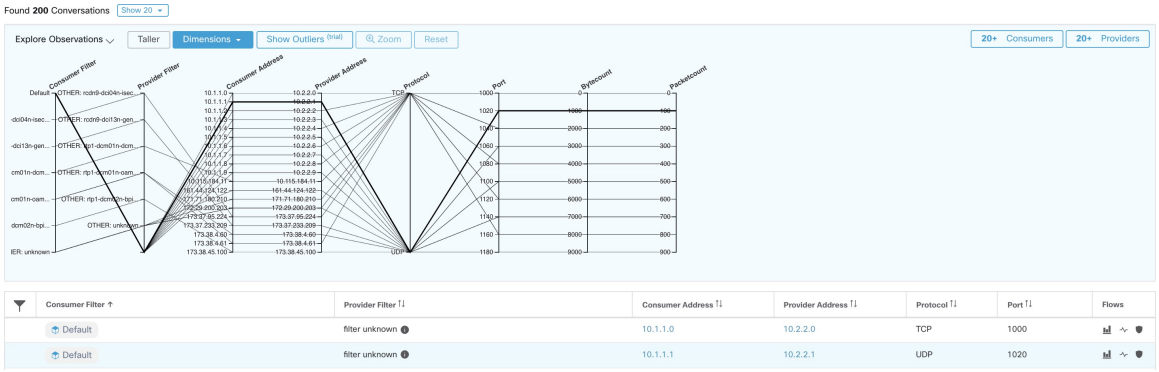
Figure 333: Explorer les observations



Observation de conversation survolée

En raison de la nature pluridimensionnelle des données des conversations, ce graphique est large par défaut et nécessite un défilement vers la droite pour le visualiser dans son intégralité. C'est pourquoi il est utile de désactiver toutes les dimensions sauf celles qui vous intéressent. La fonction de survol dans Explorer les conversations permet de mettre en correspondance (au survol) chaque conversation avec la vue de liste du tableau.

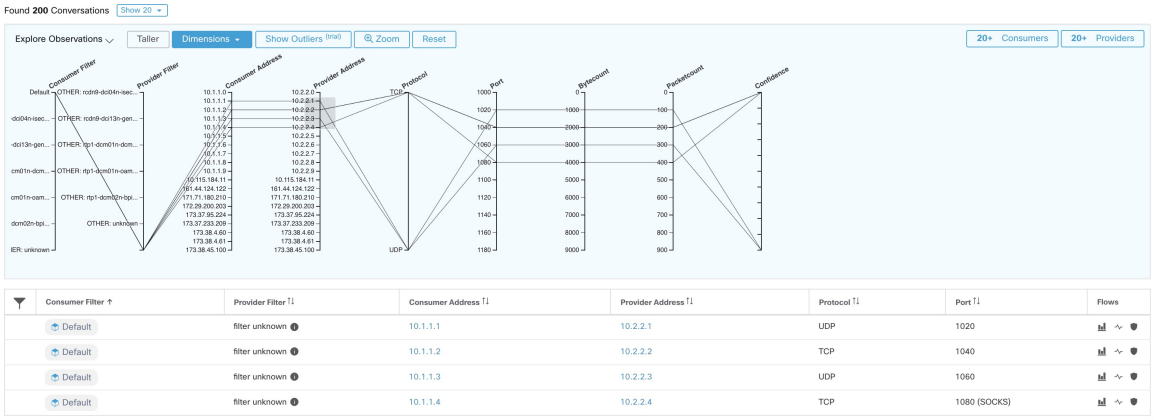
Figure 334: Observation de conversation survolée



Filtrage

Faire glisser le curseur le long de l'un des axes crée une sélection qui affichera uniquement les observations correspondant à cette sélection. Cliquez à nouveau sur l'axe pour supprimer la sélection à tout moment. Des sélections peuvent être effectuées sur n'importe quel nombre d'axes à la fois. La liste des observations sera mise à jour pour afficher uniquement les conversations sélectionnées.

Figure 335: Filtrage

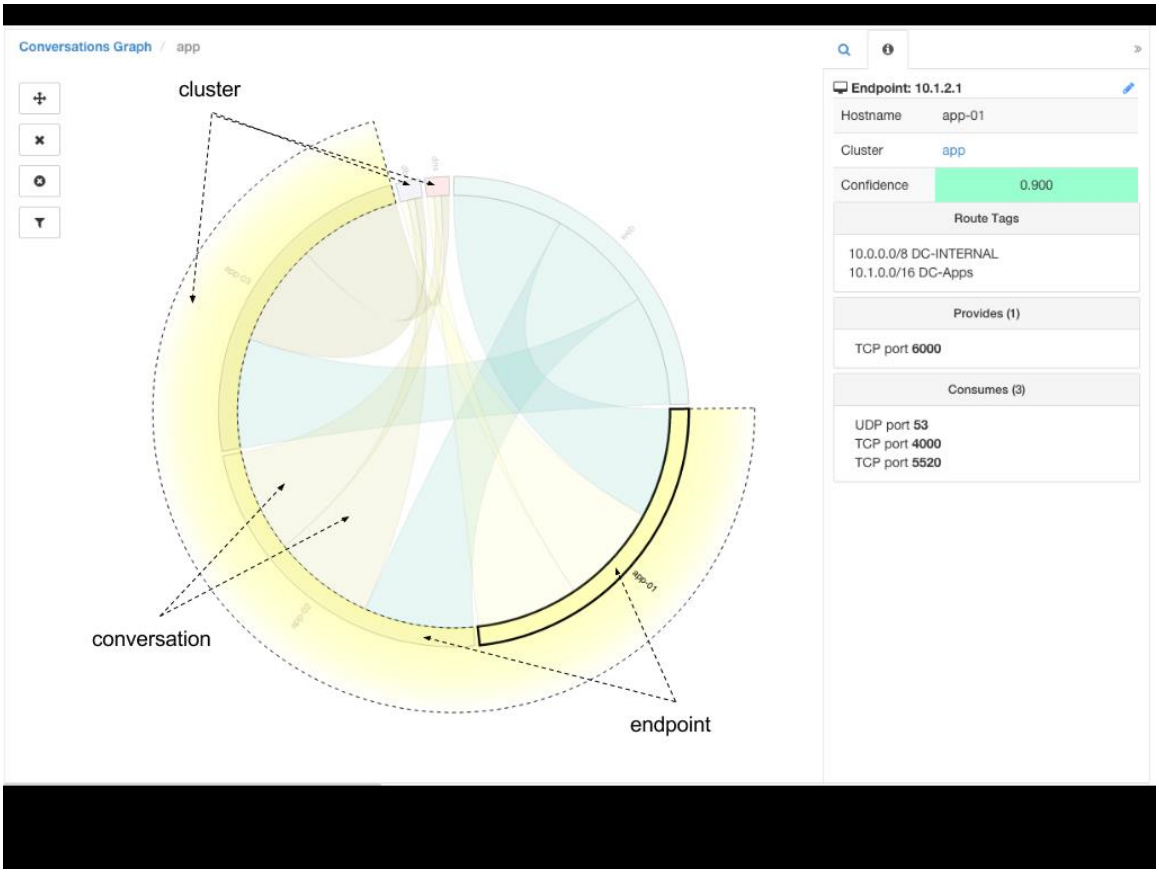


Vue graphique des conversations

La présentation du tableau des conversations est similaire à la page d'affichage des politiques, sauf qu'au lieu de se concentrer sur les partitions, grappes et politiques, elle se concentre sur les grappes/charges de travail/conversations. Comme l'illustre la figure ci-dessous, les arcs externes au niveau supérieur représentent des grappes et peuvent être développés pour afficher les hôtes membres/charges de travail comme des arcs internes. Les accords représentent les conversations ou les connexions.

Les commandes et le panneau latéral de la vue de conversation se comportent de la même manière que la vue de la politique, à l'exception du fait que les informations du panneau latéral affichent également des informations détaillées sur les charges de travail sélectionnées, telles que les services consommés/fournis, ainsi qu'un lien vers la grappe parente et des informations sur le processus, le cas échéant.

Figure 336: Vue graphique des conversations



Principaux consommateurs et fournisseurs de conversations

Le nombre de principaux consommateurs ou fournisseurs en fonction du nombre total de conversations reflétant les filtres choisis peut être consulté à partir de deux boutons en haut du tableau Conversations. Cliquez sur chacun d'eux pour voir une boîte de dialogue contenant un tableau avec la colonne Nombre de conversations ainsi que l'adresse, le nom d'hôte et d'autres colonnes annotées par l'utilisateur de chaque client ou fournisseur.

Figure 337: Au-dessus du tableau Conversations

Figure 338: Boîte de dialogue modale des principaux consommateurs

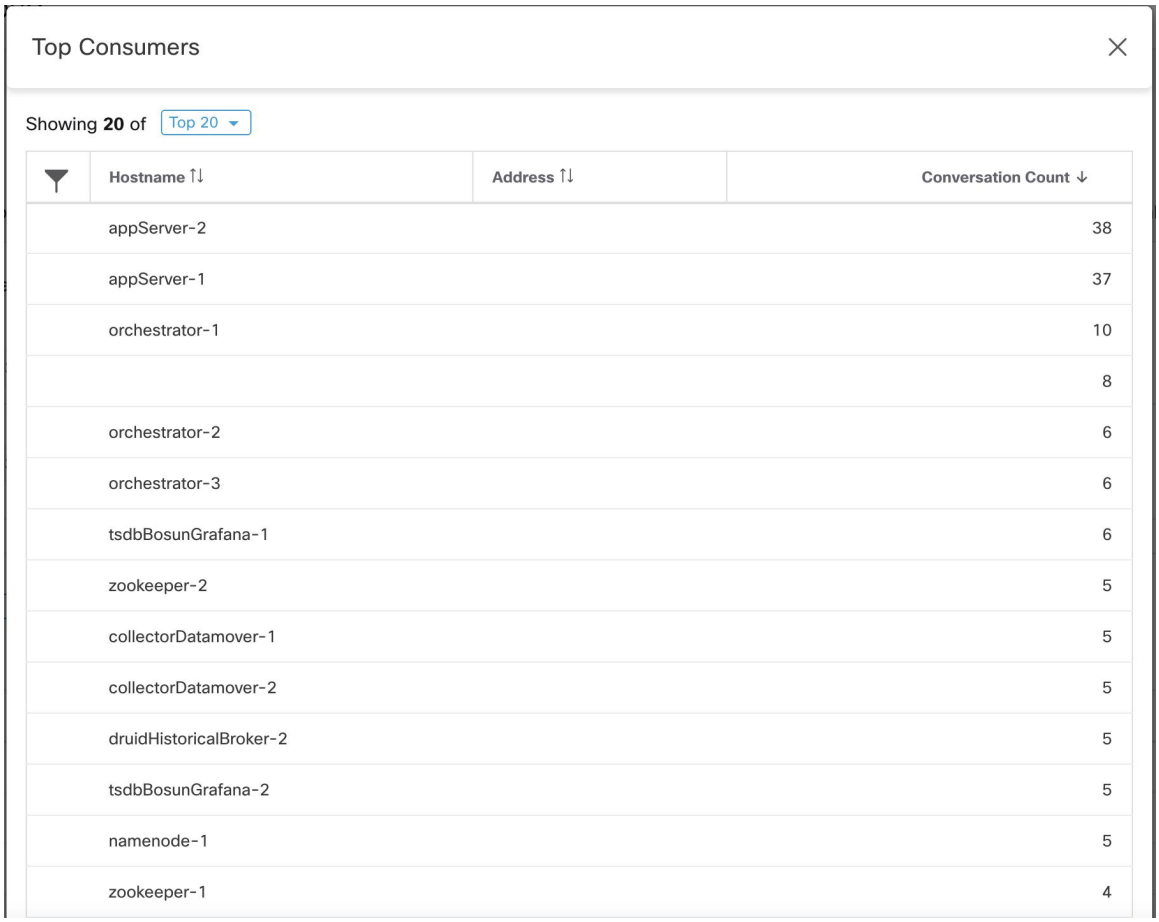
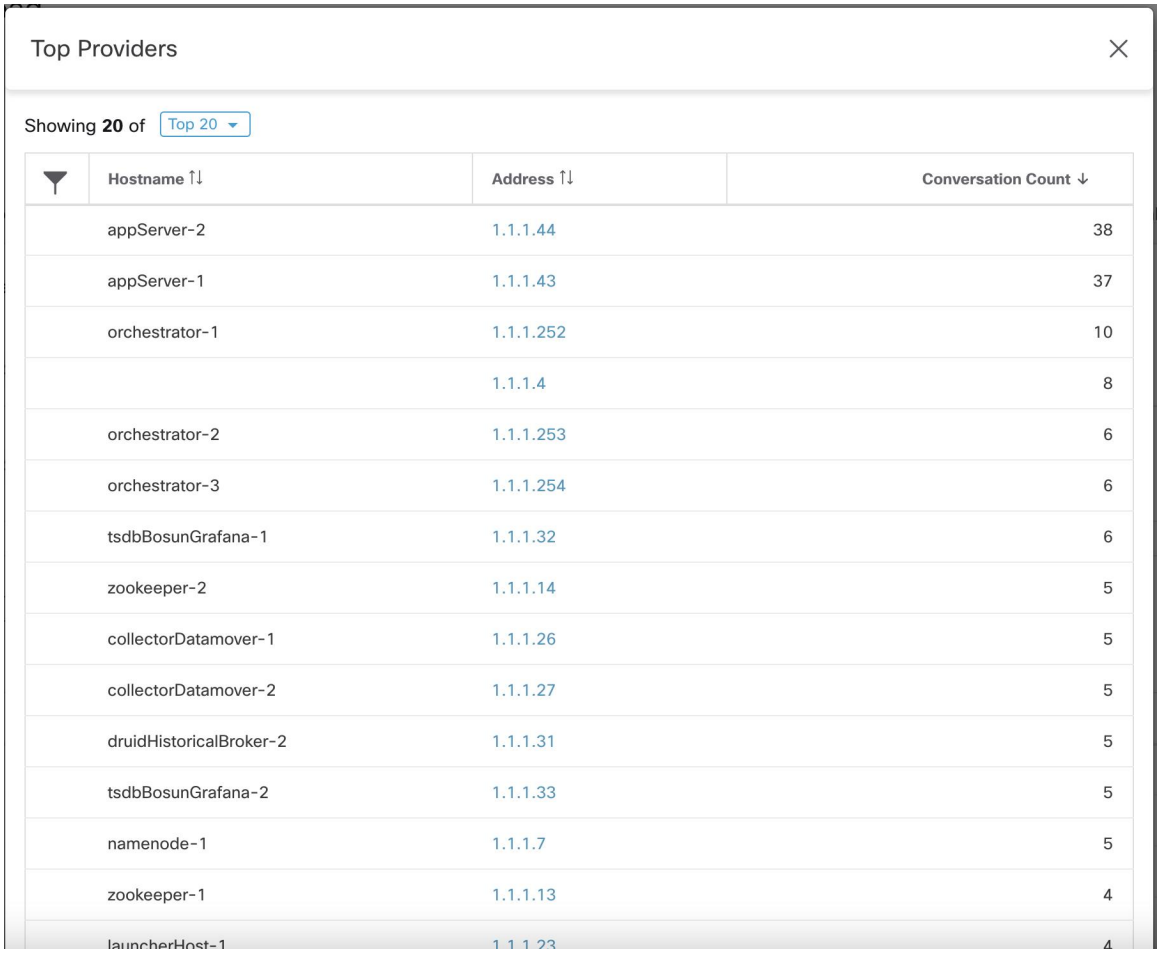


Figure 339: Boîte de dialogue modale des principaux fournisseurs



Configuration automatisée de l'équilibreur de charge pour la découverte automatique des politiques (F5 uniquement)

Important **Il s'agit d'une fonctionnalité expérimentale.**

Cette fonctionnalité et ses API sont dans la **configuration ALPHA** et sont susceptibles de changer et d'être améliorées dans les versions futures.

La découverte automatique des politiques génère ces dernières à partir de la configuration des équilibreurs de charge connectés à un orchestrateur externe. La génération de politiques à partir de la configuration réduit la dépendance à l'égard des données de flux et améliore la précision des grappes découvertes et des politiques.

Elle compte sur les clients pour transmettre les flux à l'équilibreur de charge pour générer des politiques autorisant ce trafic.

Terminologie

Adresse IP virtuelle**VIP** : adresse IP à laquelle le client envoie le trafic destiné à un service.

SNIP SNAT IP : adresse IP utilisée par l'équilibreur de charge pour envoyer le trafic aux hôtes principaux.

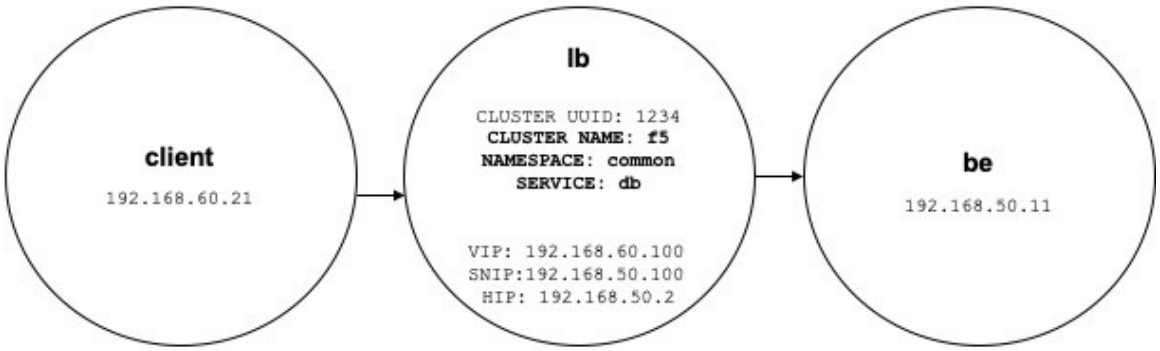
Point de terminaison Backend (principal)**BE** : adresse IP de l'hôte principal.

HIP IP de vérification de l'intégrité : adresse IP source utilisée par l'équilibreur de charge pour envoyer le trafic de vérification de l'intégrité aux hôtes principaux.

Note Les HIP sont les mêmes que les SNIP en mode automap. Cependant, les HIP et les SNIP peuvent différer lorsqu'un regroupement SNAT est configuré.

Déploiement

Figure 340: Déploiement



Envisagez le déploiement suivant dans lequel les VIP, les SNIP et les HIP de l'équilibreur de charge font partie de la portée *lb* et les BE font partie de la portée *be* . Les portées sont créées comme suit.

- Client

  La portée du client comprend les clients communiquant avec l'équilibreur de charge. Pour l'exemple ci-dessus, la requête de portée *client* est la suivante :

  ```
  address eq 192.168.60.21 or address eq 192.168.60.22
  ```

- lb

  L'orchestrateur externe F5 étiquette les VIP, les SNIP, les HIP et les BE utilisés par l'équilibreur de charge. Ces étiquettes peuvent être utilisées pour créer des requêtes de portée, où *orchestrator_system/service_name* est utilisé pour sélectionner les VIP, *orchestrator_system/service_startpoint* les SNIP, et *orchestrator_system/service_healthcheck_startpoint* des HIP pour le service. Pour l'exemple ci-dessus, une requête de portée qui inclut les VIP, les SNIP et les HIP pour la *base de données* de service est la suivante :

  ```
  user_orchestrator_system/cluster_id eq 1234 and
  (user_orchestrator_system/service_name eq db or
  user_orchestrator_system/service_startpoint eq db or
  user_orchestrator_system/service_healthcheck_startpoint eq db)
  ```

Note Les SNIP et les VIP doivent se trouver dans la même portée.

- Être

  user_orchestrator_system/service_endpoint sélectionne les environnements de base (BE) pour un service. Pour l'exemple ci-dessus, une requête de portée qui inclut des éléments BE pour la *base de données de service* est la suivante :

```
user_orchestrator_system/cluster_id eq 1234 and
user_orchestrator_system/service_endpoint eq db
```

Grappes

Chaque service génère jusqu'à quatre grappes découvertes, dont seule la grappe de service est visible pour l'utilisateur. Les grappes SNIP, HIP et BE apparaissent comme des grappes connexes pour la grappe de service. Les grappes HIP et BE sont générées uniquement lorsque des HIP et des BE sont présents dans la portée *lb*.

Pour l'exemple ci-dessus, la découverte automatique des politiques génère une grappe SNIP et une grappe HIP dans la portée *lb* qui incluent les SNIP et les HIP pour le service. Étant donné que les environnements BE se trouvent en dehors de la portée *lb* , la découverte automatique des politiques ne génère pas de grappe principale, mais ajoute la portée *be* à la liste des grappes associées à *db*.

Les grappes sont générées comme suit :

- Service

  La grappe de service comprend des VIP pour le service. La requête pour la grappe de services est la suivante :

```
user_orchestrator_system/cluster_id eq 1234 and
user_orchestrator_system/namespace eq common and
user_orchestrator_system/service_name eq db
```

- SNIP

  Les SNIP pour un service sont inclus dans la grappe SNIP. La requête pour la grappe SNIP est la suivante :

```
user_orchestrator_system/cluster_id eq 1234 and
user_orchestrator_system/service_startpoint eq db
```

- HIP

  Les HIP d'un service sont inclus dans la grappe HIP. La requête pour la grappe HIP est la suivante :

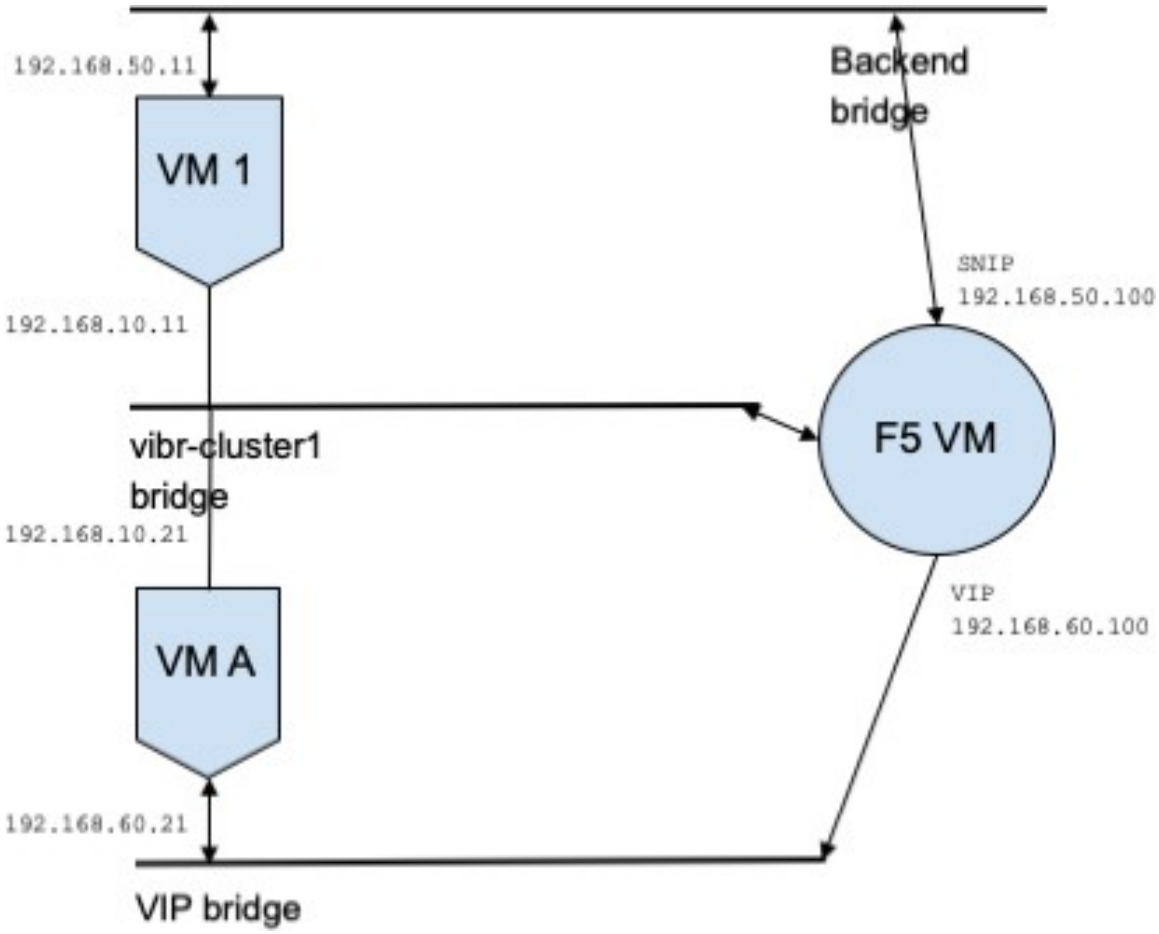
```
user_orchestrator_system/cluster_id eq 1234 and
user_orchestrator_system/service_healthcheck_startpoint eq db
```

- Backend (Système principal)

  Une grappe principale du service est générée lorsqu'un ou plusieurs BE font partie de la portée *lb*. Cela ne s'applique pas à l'exemple ci-dessus, ce qui signifie qu'aucune grappe principale n'est générée dans la portée *lb*.

Politiques

Figure 341: Génération de politiques



Supposons que nous ayons une *base de données* de service avec VIP *192.168.60.100*, SNIP *192.168.50.100* et une machine virtuelle principale avec l'adresse IP *192.168.50.11* à l'écoute sur le port 10000. Le trafic de la VM cliente *192.168.60.21* vers la *base de données* entraîne les politiques suivantes :

- Politique du client à la VIP.

  La politique suivante permet à la machine virtuelle cliente d'accéder au service *db*.

```
{
"src": "<uuid of client scope>",
"dst": "<uuid of service cluster>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
]
}
```

- Politique de SNIP à BE.

  Une politique autorisant le trafic de SNIP vers BE est générée automatiquement à partir de la configuration et apparaît comme politique associée pour *db*.

```
{
"src": "<uuid of SNIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
10000,
10000
],
"proto": 6,
}
]
```

  Un connecteur de politique de la portée *lb* vers la portée *be* transmet la politique suivante vers celle-ci.

Consommateurs	Fournisseur	Port	Protocole	Action
SNIP	à	10 000	TCP	Autoriser

  Cela génère des règles de pare-feu sur l'hôte BE 192.168.50.11, autorisant le trafic entrant de LB SNIP 192.168.50.100 sur le port 10000.

- Politiques de HIP à BE.

  Une politique autorisant le trafic du HIP vers BE est générée automatiquement à partir de la configuration et apparaît comme politique associée pour *db*.

```
{
"src": "<uuid of HIP cluster>",
"dst": "<uuid of be scope>",
"l4_params": [
{
"port": [
0,
0
],
"proto": ICMP,
}
]
}
```

  Un connecteur de politique de la portée *lb* vers la portée *be* transmet la politique suivante vers celle-ci.

Consommateurs	Fournisseur	Port	Protocole	Action
HIP	à	0	ICMP	Autoriser

  Cela génère des règles de pare-feu sur l'hôte BE *192.168.50.11* , autorisant le trafic ICMP entrant de LB HIP *192.168.50.2*.

Mises en garde

- Lorsque plusieurs services de la même instance d'équilibreur de charge portent le même nom, les règles principales générées pour ces services comprendront les pools de serveurs principaux, c.-à-d. les règles seront plus permissives que nécessaire.

Serveur de publication des politiques

Le serveur de publication des politiques est une fonctionnalité Cisco Cisco Secure Workload avancée qui permet à un fournisseur tiers de mettre en œuvre ses propres algorithmes de mise en application, qui sont optimisés pour les appareils réseau tels que les équilibreurs de charge ou les pare-feu. Cette fonctionnalité est réalisée en publiant les politiques définies sur une instance Kafka résidant dans la grappe Cisco Secure Workload et en fournissant aux clients des certificats client Kafka, ce qui permet au code du fournisseur tiers de récupérer les politiques Kafka et de les traduire correctement dans la configuration de leurs appareils réseau.

Cette section vise à décrire la procédure que les fournisseurs tiers, en abrégé les utilisateurs dans ce qui suit, doivent suivre pour exploiter la fonctionnalité de *serveur de publication des politiques* avec Java sur Linux.

Prérequis

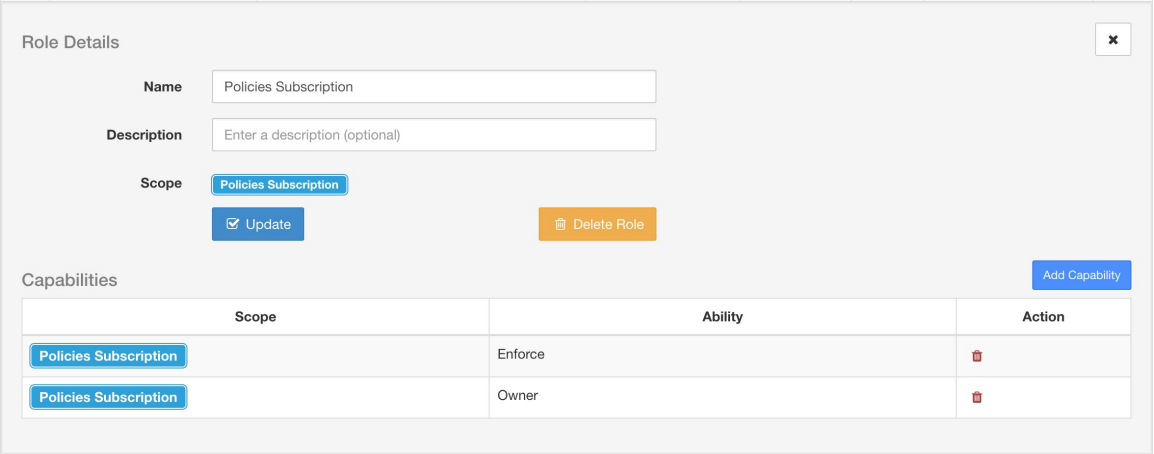
Les progiciels suivants sont installés sur un système Linux, tel qu'Ubuntu 16.04.

- JDK Java 8
- Clients Apache Kafka : kafka-clients-1.0.0.jar
- Tampons du protocole, base : protobuf-java-3.4.1.jar
- Apache Log4j : log4j-1.2.17.jar
- Façade de journalisation simple pour Java : sLF4j-api-1.7.25.jar, sLF4j-log4j12-1.7.25.jar
- Compresseur/décompresseur Snappy pour Java : Snappy-java-1.1.4.jar

Obtention des certificats client Kafka

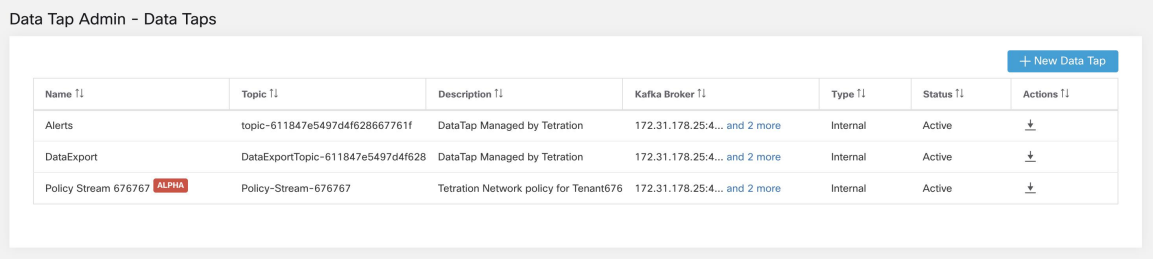
- Créez un rôle d'utilisateur avec la capacité « *Propriétaire* » et attribuez-le au compte d'utilisateur de votre choix :

Figure 342: Configuration des rôles d'utilisateurs pour recevoir les politiques Kafka



- Effectuez l'application des politiques comme décrit dans la section Appliquer des politiques. Cette première étape est nécessaire, car elle crée une rubrique Kafka associée à une portée active.
- Accédez à **Manage(Gestion) > Data Tap Admin (Administration des surveilleurs de données)**
- Sélectionnez l'onglet *« Data Taps »* (Dérivations de données) et téléchargez les certificats clients Kafka en cliquant sur le bouton de téléchargement sous la colonne *« Actions »*. Assurez-vous de sélectionner le format *Java Keystore* dans la boîte de dialogue de téléchargement.

Figure 343: Affichage des dérivations de données



- Le fichier de certificats clients téléchargé porte généralement un nom comme *Policy-Stream-10-Policies-Subscription.jks.tar.gz*. Créez un répertoire et décompressez-le sous ce dernier, comme indiqué ci-dessous :

```
    mkdir Policy-Stream-10-Policies-Subscription
    tar -C Policy-Stream-10-Policies-Subscription -zxf
Policy-Stream-10-Policies-Subscription.jks.tar.gz
```

Fichier de définition Protobuf

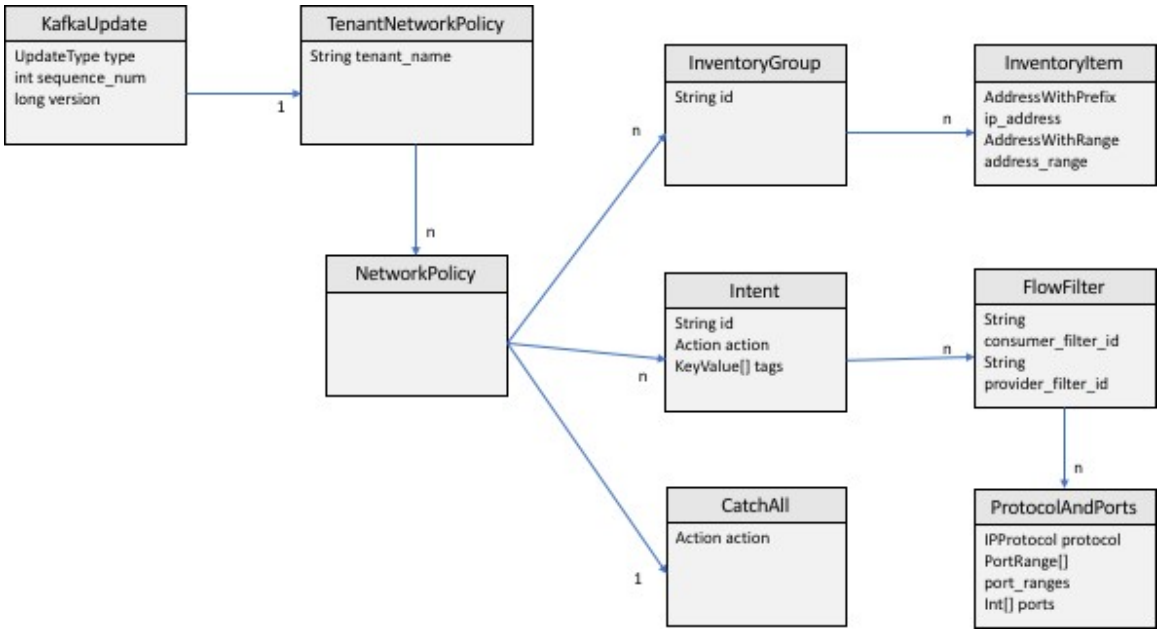
Les politiques de réseau exposées par le serveur principal Cisco Secure Workload à Kafka sont codées au format Tampons de protocole de Google. Consultez ce guide pour obtenir des instructions sur la façon de le télécharger et de l'installer sur votre système Linux.

Le fichier protocole de la politique de réseau Cisco Secure Workload peut être téléchargé ici.

Modèle de données de la politique réseau Cisco Secure Workload

L'image ci-dessous montre un diagramme UML simplifié des entités Cisco Secure Workload accessibles à Kafka :

Figure 344: Modèle de données de la politique réseau Cisco Secure Workload



Une *Cisco Secure Workload politique réseau* telle que modélisée dans protobuf se compose d'une liste de *groupes d'inventaire*, d'une liste d'*intents* et d'une politique *CatchAll* (Collectrice). Chaque politique contient tous les éléments appartenant à une portée racine. Un *InventoryGroup* contient une liste d'*InventoryItems*, qui représentent des entités Cisco Secure Workload telles que des serveurs ou des appareils en spécifiant leur adresse réseau, qu'il s'agisse d'une adresse réseau unique, d'un sous-réseau ou d'une plage d'adresses. Un *intent* décrit une action (autoriser ou refuser) à entreprendre lorsqu'un flux réseau correspond au groupe d'inventaire du consommateur *InventoryGroup*, *du fournisseur*, ainsi que les protocoles et ports réseau. *CatchAll* représente l'action globale définie pour la portée racine dans Cisco Secure Workload. Si aucun espace de travail avec application activée n'existe pour la portée racine, la politique par défaut *ALLOW* est inscrite dans la politique produite.

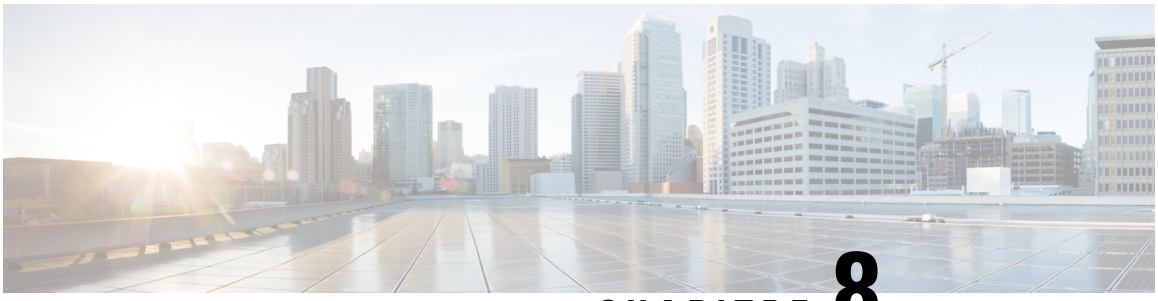
Lorsqu'une application est déclenchée par les utilisateurs ou par un changement de groupes d'inventaire, le serveur principal Cisco Secure Workload envoie un instantané complet des politiques de réseau définies à Kafka sous la forme d'une séquence de messages représentés par *KafkaUpdates*. Reportez-vous aux commentaires *KafkaUpdate* dans le fichier *tetration_network_politique.proto* pour savoir comment reconstituer ces messages en un instantané complet et comment gérer les conditions d'erreur.

Si la taille du message *KafkaUpdate* est supérieure à 10 Mo, le serveur principal Cisco Secure Workload divise ce message en plusieurs fragments, chacun de 10 Mo. S'il y a plusieurs fragments, seul le premier fragment comporte le champ *ScopeInfo* de *TenantNetworkPolicy*. *ScopeInfo* sera mis à zéro dans les fragments restants du message *KafkaUpdate*.

Mise en œuvre de référence d'un client de politiques de réseau Cisco Secure Workload.

Pour obtenir des instructions sur la mise en œuvre et des instructions sur la façon de compiler et d'exécuter un client de démonstration, consultez tnp-enforcement-client dans Java.

Cette implémentation fournit un code commun pour lire les politiques réseau du flux de politique Cisco Secure Workload via Kafka uniquement. Le code propre au fournisseur pour programmer les politiques réelles sur un périphérique réseau peut être intégré en mettant en œuvre l'interface requise PolicyEnforcementClient.



CHAPITRE 8

Configurer et surveiller les événements criminalistiques

L'ensemble de fonctionnalités **criminalistiques** permet de surveiller et d'envoyer des alertes pour d'éventuels incidents de sécurité en capturant les événements criminalistiques en temps réel et en appliquant des règles définies par l'utilisateur. Plus précisément, il permet la :

- Définition de règles pour préciser les événements d'intérêt criminalistique
- Définition des actions de déclencheur pour les événements criminalistiques correspondants
- Recherche d'événements criminalistiques spécifiques
- Visualisation des processus générateurs d'événements et leurs lignages complets

Avertissement Lorsque la fonction d' **criminalistique** est activée, les agents logiciels peuvent avoir besoin de ressources de l'hôte supplémentaires en fonction de la configuration de l'agent. Consultez la section de configuration de l'agent logiciel.

Compatibilité

Les signaux criminalistiques sont rapportés par les agents de visibilité en profondeur sur toutes les plateformes, à l'exception de Solaris. Actuellement, seuls quelques signaux criminalistiques sont pris en charge par AIX. Pour en savoir plus, consultez la section Signaux .criminalistiques

Les renseignements criminalistiques sont fournis par le biais des API du noyau Linux, d'audit et du journal système, les API du noyau Windows, les événements Windows, le système d'audit AIX et autres. En général, les fournisseurs de systèmes d'exploitation garantissent la compatibilité au sein d'une version majeure. Toutefois, il est possible que les API diffèrent légèrement d'une plateforme à l'autre et d'une version mineure à l'autre, car les fournisseurs de systèmes d'exploitation peuvent reporter des fonctionnalités et des correctifs. Par conséquent, certains types d'événements d'criminalistiques peuvent ne pas être disponibles sur certaines plateformes. De plus, l'agent ne tente pas de récupérer ou d'activer les services de système d'exploitation désactivés au démarrage de l'agent.

Par exemple, il existe un certain nombre de signaux criminalistiques qui utilisent le cadre d'audit Linux. Si la criminalistique est activée, un agent de visibilité approfondie insère des règles d'audit Cisco Secure Workload dans le système après le démarrage de l'agent. L'insertion de règle nécessite que le système ait l'utilitaire augenrules installé et le répertoire /etc/audit/rules.d. Si l'une de ces conditions préalables n'est pas remplie, les règles d'audit Cisco Secure Workload ne seront pas insérées. Par conséquent, les signaux criminalistiques, y compris l'accès aux fichiers et la création de sockets bruts, ne seront pas signalés.

Si un utilisateur a activé la fonction criminalistique précédemment et la désactive, l'agent supprime les règles d'audit qui sont insérées par Cisco Secure Workload. Sur Red Hat 7.3 et CentOS 7.3, nous avons observé un bogue du système d'exploitation qui pourrait avoir une incidence sur le processus de suppression de règles. L'agent supprime les règles d'audit en : 1. Suppression du fichier taau.rules dans le dossier */etc/audit/rules.d/* 2. Exécution de *$service auditd restart*. Le système d'exploitation régénère l'ensemble de règles en fonction des fichiers *audit.rules* et **.rules* dans */etc/audit/rules.d/*. Ensuite, auditd chargera les règles dans le système.

Le système d'exploitation ajoute *-D* au début du fichier /etc/audit/rules.d/audit.rules pour effacer toutes les règles avant d'insérer le nouvel ensemble de règles. Cependant, sur les machines Red Hat 7.3 et CentOS 7.3, le fichier */etc/audit/rules.d/audit.rules* peut ne pas comporter *-D*. En effet, le système d'exploitation crée un fichier vide */etc/audit/rules.d/audit.rules* si ce fichier n'existe pas et un fichier de règles par défaut dans le sous-répertoire */usr/watch/doc/audit-* <version> / s'il n'existe pas non plus. Par exemple, */usr/share/doc/audit-2.8.4/rules/10-base-config.rules* est un emplacement possible par défaut pour les règles. Le comportement exact du système d'exploitation peut être observé à partir du script de mise à jour de RPM en exécutant *$rpm-qf-scripts/etc/audit/rules.d*

Sous Linux, certains signaux criminalistiques reposent sur l'observation d'appels systèmes 64 bits. Les appels système Linux 32 bits ne sont pas pris en charge dans la version actuelle.

Signaux criminalistiques

La fonction **Forensics** (Criminalistique) doit être activée pour que les agents logiciels puissent saisir et signaler les événements criminalistiques. La fonction peut être activée dans la configuration de l'agent logiciel. Pour en savoir plus, consultez la section Configuration de l'agent logiciel.

Lorsque la fonction **Forensics** (Criminalistique) est activée, l'agent signale les événements criminalistiques suivants.

Signal	Description
Escalade de privilèges	Les escalades de privilèges, telles que les commandes exécutées avec sudo.
Connexion de l'utilisateur	Événements de connexion de l'utilisateur.
Échec de connexion de l'utilisateur	Les tentatives de connexion de l'utilisateur qui ont échoué
Shellcode	Les exécutions de shell suspectes ressemblant à des tentatives de code shell
Accès au fichier	L'accès aux fichiers sensibles tels que les fichiers de mots de passe.
Compte d'utilisateur	L'ajout ou la suppression de comptes utilisateur
Commande non vue	Les nouvelles commandes que l'agent n'a pas vues. Les utilisateurs peuvent utiliser la note d'anomalie de commande pour ajuster les résultats en fonction de la portée. Consultez la section Commande non vue pour plus de détails.
Bibliothèque non vue	La nouvelle bibliothèque que l'agent n'a pas encore vu fonctionner et qui a été chargée auparavant.
Création d'interface de connexion brute	Les processus créant des sockets bruts. Par exemple, le port knocking (frappe).
Fichier binaire modifié	Les modifications apportées aux valeurs de condensé ou aux heures de modification de fichiers binaires connus.
Bibliothèque modifiée	Les modifications apportées aux valeurs de condensé ou aux heures de modification de bibliothèques connues.
Canaux auxiliaires	Les tentatives d'attaques par canal auxiliaire (Meltdown).
Suivre la connexion de l'utilisateur	Les processus descendants qui bifurquent ou s'exécutent après les événements de connexion.
Suivre le processus	Les événements de processus de suivi signalent les processus qui correspondent aux règles de configuration criminalistique de l'utilisateur en fonction des attributs de processus tels que le chemin binaire, la chaîne de commande, etc.
Anomalie de réseau	Pour les anomalies de trafic réseau du charge de travail, consultez Détection des anomalies de réseau basée sur le PCR pour en savoir plus.

Table 31: Signaux criminalistiques pris en charge sur AIX

Signal	Description
Escalade de privilèges	Les escalades de privilèges, telles que les commandes exécutées avec sudo.
Création d'interface de connexion brute	Les processus créant des sockets bruts. Par exemple, le port knocking (frappe).
Compte d'utilisateur	L'ajout ou la suppression de comptes utilisateur

Escalade de privilèges

Lorsque le processus fait passer son privilège de faible à élevé, ceci est considéré comme une escalade de privilèges. Sous Linux, cela signifie que l'ID utilisateur du processus est passé de non nul à nul. Il existe des cas légitimes tels que la modification du mot de passe d'un utilisateur ordinaire et d'autres programmes binaires à usage spécial tels que Sudo. Cet événement n'est actuellement pas disponible dans Windows. L'escalade de privilèges dans Windows se fait généralement par d'autres mécanismes plutôt que par la modification des privilèges du processus lui-même, c'est-à-dire le niveau d'intégrité. Les escalades de privilèges sur Windows sont couvertes par d'autres types d'événements criminalistiques, tels que des commandes ou des modifications binaires non vues.

Connexion de l'utilisateur

L'utilisateur se connecte aux événements, y compris SSH, RDP et d'autres types de connexions. Chaque fois que cela est possible, les capteurs permettent de savoir qui, quand et comment un utilisateur se connecte. Par exemple, pour SSH sous Linux, les capteurs indiquent le nom d'utilisateur, le type d'authentification (mot de passe, public) et l'adresse IP source.

Échec de connexion de l'utilisateur

Comme pour les événements de connexion de l'utilisateur ci-dessus, les capteurs signalent l'échec des tentatives de connexion avec des informations similaires lorsqu'elles sont disponibles.

Shellcode

Les événements de shellcode ont des interprétations différentes sous Linux et Windows. Sous Linux, les capteurs identifient les processus s'exécutant en tant qu'interface Shell interactive sans session de connexion ni point terminal. (Il n'y a aucune raison réelle pour qu'un shell interactif s'exécute en dehors d'une session de connexion). Dans cette version, la détection des événements de shellcode est limitée, car elle suppose que l'attaque utilisera un shell déjà disponible dans le système. Si une attaque télécharge de nouveaux fichiers binaires, les capteurs signalent ces fichiers binaires soit comme des commandes non vues, soit comme des modifications binaires, s'ils remplacent des fichiers binaires existants. Dans Windows, chaque processus lié à la DLL PowerShell sera étiqueté comme shellcode. Les utilisateurs peuvent créer des règles pour filtrer les dossiers légitimes.

Accès au fichier

Les événements d'accès aux fichiers signalent les accès aux fichiers sensibles, tels que les fichiers de mots de passe. Dans cette version, la liste des fichiers à surveiller ne peut pas être modifiée par les utilisateurs. Sous Linux, le capteur surveille l'accès en écriture au dossier /etc/passwd. Le capteur surveille également les accès en lecture et en écriture au dossier /etc/shadow. Windows ne déclenchera pas cet événement dans cette version.

Compte d'utilisateur

Les événements de comptes d'utilisateurs signalent la création de comptes d'utilisateurs locaux chaque fois que les informations sont disponibles.

Commande non vue

Les événements de commandes non vue signalent des commandes que le capteur n'a pas encore vues. Une commande non vue est définie comme une transition ou une périphérie non vue d'un processus parent à un processus enfant. Par exemple, en supposant qu'un serveur Web (httpd) exécute un script CGI appelé abc.sh, lorsque le capteur le verra pour la première fois, il signale abc.sh comme une commande non vue. Les exécutions ultérieures de abc.sh par le serveur Web n'entraîneront pas d'événements criminalistique, car le capteur l'a déjà vu et signalé. Si un service ou un processus n'exécute jamais de fichier binaire, un événement de commande non vue de ce service ou processus indique une dégradation malveillante possible. Notez que les capteurs sont sans état au redémarrage, donc une commande vue précédemment sera à nouveau signalée après le redémarrage du capteur.

À partir de la version 3.4, pour les grappes de logiciels-services, chaque événement de commande non vue est associé à un score d'anomalie de commande allant de 0.0 à 1.0. Plus la note est faible, plus la transition est anormale. Les transitions de commande, c'est-à-dire les n-uplets (ligne de commande parente, ligne de commande) font l'objet d'une vérification croisée pour détecter les transitions anormales parmi les événements ayant le même n-uplet ci-dessous :

- Les portées les plus étroits auxquels le capteur appartient. Par exemple, l'événement de commande non vue est observé sur la charge de travail W qui appartient aux lignages de portée suivants :: `Portée racine -> A -> B -> C et Portée racine -> D -> E`. Ensuite, la commande est recoupée par rapport à toutes les charges de travail des portées C et E (à noter que C et E peuvent se chevaucher ou non). La note d'anomalie de l'événement est le maximum des notes d'anomalie de l'événement en ce qui concerne ces 2 portées.
- Chemin d'exécution du processus en cours d'exécution.
- Le chemin d'exécution du processus parent.
- Le condensé binaire du processus en cours d'exécution.

Une note de 1.0 signifie que la même transition de commande ayant le même nuplet `(portée la plus étroite, chemin d'exécution, chemin d'exécution parent, condensé binaire)` a été observée. Une note de 0.0 signifie qu'une transition de commande avec un tel chemin d'exécution, le chemin d'exécution parent et le condensé binaire du processus en cours n'a jamais été observée sur des hôtes des mêmes portées. La note d'anomalie peut être utilisé pour supprimer le déclenchement d'alertes de commandes non vues similaires dans la même portée et réduire les faux positifs. Consultez Règles Cisco Secure Workload par défaut pour obtenir un exemple de la façon dont cette note peut être utilisée.

Note Le score d'anomalie est uniquement disponible pour les grappes de logiciels-services à partir de la version 3.4.

Bibliothèque non vue

Les événements de bibliothèque non vue signalent les bibliothèques pour lesquelles le capteur n'a pas vu de processus téléversé auparavant. Une bibliothèque non vue est définie comme une paire non visible de chemin d'exécution binaire et de chemin de bibliothèque. Par exemple, une application téléverse généralement une liste de bibliothèques relativement stable. Un attaquant qui a accès à la machine peut redémarrer l'application et les bibliothèques malveillantes LD_PRELOAD. Lorsque le capteur détecte les bibliothèques malveillantes nouvellement téléversées dans le chemin d'exécution binaire de cette application pour la première fois, il signale des événements de bibliothèque non vue. Les chargements ultérieurs des bibliothèques malveillantes n'entraîneront pas d'événements criminalistique, car le capteur les a déjà vus et signalés. Les cas légitimes comprennent l'application qui téléverse de nouvelles bibliothèques après la mise à niveau ou les applications qui téléversent dynamiquement de nouvelles bibliothèques. Notez que les capteurs peuvent signaler à nouveau une bibliothèque vue précédemment après le redémarrage.

Notez qu'il s'agit d'une fonctionnalité expérimentale et susceptible de changer dans les versions futures.

Création d'interface de connexion brute

Les événements de création d'interface de connexion (socket) brute ne sont pris en charge que sur cette version. Les sockets bruts sont généralement utilisés pour surveiller ou injecter / usurper le trafic. Il y a des utilisations légitimes des sockets bruts, par exemple dans les outils de diagnostic comme tcpdump, ou lors de la création de paquets IP spéciaux comme ping ou aRP. Les utilisations malveillantes incluent les analyses furtives pour éviter la journalisation par machines cible / victime, les programmes malveillants de port d'accès, etc. Les capteurs Cisco Secure Workload créent également des sockets bruts pour collecter des informations relatives au flux. (Par souci de cohérence, les capteurs ne suppriment pas les événements déclenchés par leur propre collecte d'informations de flux).

Fichier binaire modifié

Les événements binaires modifiés signalent les modifications apportées au contenu du fichier et aux attributs des fichiers binaires pour les processus en cours d'exécution. Les capteurs enregistrent les attributs de fichier de chaque processus en cours d'exécution. Si un processus exécute un fichier binaire dans le même chemin, mais avec des attributs de fichier différents (ctime, mtime, taille ou condensé), le capteur signale le processus comme modification de fichier binaire. Les cas légitimes comprennent la mise à niveau de l'application.

Bibliothèque modifiée

Les événements de modification de bibliothèque signalent les modifications apportées au contenu et aux attributs du fichier des bibliothèques pour les processus en cours d'exécution. Les capteurs enregistrent les attributs de fichier des bibliothèques chargées. Si un processus charge une bibliothèque par le même chemin, mais avec des attributs de fichier différents (ctime, mtime, taille ou condensé), le capteur signalera le processus come ayant subi une modification de bibliothèque. Les cas légitimes comprennent la mise à niveau de la bibliothèque.

Notez qu'il s'agit d'une fonctionnalité expérimentale et susceptible de changer dans les versions futures.

Canaux auxiliaires

Les événements des canaux auxiliaires signalent l'exécution de logiciels qui exploitent les vulnérabilités de ces derniers. Cette version fournit une capacité de détection de canal auxiliaire unique sur une plateforme Linux sélectionnée : la fusion (Meltdown). Consultez les détails ci-dessous pour connaître les configurations de machines prises en charge. Il s'agit de fonctionnalités de sécurité avancées qui sont donc désactivées par défaut. Les utilisateurs doivent s'attendre à une augmentation de l'utilisation du processeur lorsque la création de rapports sur les canaux auxiliaires est activée. Le quota de CPU configuré dans l'interface utilisateur sera toujours respecté. Si le sous-processus de collecte criminalistique du capteur détermine que son utilisation du processeur est trop élevée pendant trop longtemps, il s'arrête et le processus du capteur parent le redémarre avec un léger délai. L'activation de cette fonctionnalité sur des noyaux anciens ou non pris en charge pourrait entraîner une instabilité du système. Il est recommandé d'effectuer des tests dans des environnements similaires hors production.

Cette fonctionnalité peut être activée/désactivée à partir de la page de configuration de l'agent dans l'interface utilisateur et dans le profil de configuration de chaque agent.

La fusion (Meltdown) est une attaque de canal auxiliaire qui utilise abusivement les fonctionnalités d'exécution supposée et de mise en cache du processeur (https://meltdownattack.com/). Elle permet à un attaquant de lire les données du domaine privilégié à partir d'un domaine non privilégié, par exemple, la lecture de la mémoire du noyau d'une application de l'espace utilisateur sans privilèges d'anneau 0. La détection de la fusion prend actuellement en charge CentOS 7 et Ubuntu 16.04.

Suivre la connexion de l'utilisateur

Les événements de suivi de connexion d'utilisateur signalent les processus descendants (jusqu'à 4 niveaux) qui sont exécutés après un processus d'événement de connexion d'utilisateur (SSH, RDP, etc.). Les processus signalés dans le cadre de cet événement de suivi de connexion de l'utilisateur le sont à des fins d'audit et n retranscrivent pas nécessairement d'événements de sécurité.

Suivre le processus

Les événements de suivi de processus signalent les processus qui correspondent aux règles de configuration criminalistique de l'utilisateur en fonction des attributs de processus tels que le chemin binaire, la chaîne de commande, etc. Les processus signalés dans le cadre de cet événement de suivi du processus le sont à des fins d'audit et ne comportent pas nécessairement d'événements de sécurité.

Exemple 1 : processus de rapport exécutés par cmd.exe ou powershell.exe

Event Type = Follow Process AND (Process Info - Exec Path contains cmd.exe OR Process Info - Exec Path contains powershell.exe)

Exemple 2 : Indiquer tous les processus créés par winword.exe, excel.exe ou powerpnt.exe.

Event Type = Follow Process with_ancestor (Process Info - Exec Path contains winword.exe OR Process Info - Exec Path contains excel.exe OR Process Info - Exec Path contains powerpnt.exe)

Remarque : Les événements de suivi du processus peuvent être suivis par l'un des signaux de processus suivants :

- Process Info - Exec Path

- Process Info - Command String
- Process Info - Username
- Follow Process - Parent Exec Path
- Follow Process - Parent Command String
- Follow Process - Parent Username

Configuration criminalistique

La fonction criminalistique utilise une configuration basée sur les intents. Les intents spécifient comment appliquer les profils criminalistiques aux filtres d'inventaire. Le profil criminalistique se compose de plusieurs règles criminalistiques. Les profils d'un intent sont appliqués dans l'ordre, de haut en bas.

Règles criminalistiques

Note Le nombre maximal de règles par portée racine est de 100.

Ajout d'une règle criminalistique

Cette section explique comment ajouter de nouvelles règles criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

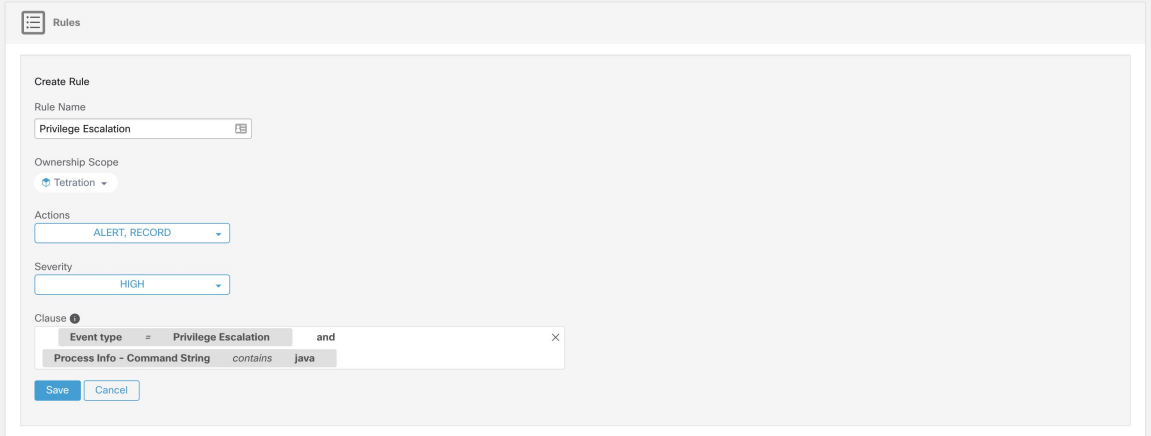
Étape 2 Cliquez sur **Create Rule** (créer une règle).

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom de la règle	Entrez un nom pour la règle. Le nom ne peut pas être vide
Portée de la propriété	Saisissez une portée de propriété pour cette règle.

Champ	Description
Actions	Sélectionnez des actions lorsque cette règle est déclenchée. **Record**(Enregistrement) : signifie que les événements de sécurité correspondants persistent pour une analyse plus approfondie. L'action d'**alerte** signifie la publication des événements de sécurité correspondants dans le système d'alerte Cisco Secure Workload.
Gravité	Sélectionnez le niveau de gravité de cette règle : **LOW**(FAIBLE), **MEDIUM**(MOYEN), **HIGH**(ÉLEVÉ), **CRITICAL**(CRITIQUE) ou **REQUIRES IMMEDIATE ACTION** (NÉCESSITE UNE ACTION IMMÉDIATE)
Article	Saisissez une clause de règle. Une clause doit contenir des signaux d'événement de sécurité provenant d'un événement criminalistique de processus ou d'un événement de charge de travail. Une clause n'est pas valide si elle contient à la fois des signaux de processus et de charge de travail.

Figure 345: Créer une règle



Étape 4 Cliquez sur **Save** (enregistrer).

Composition des règles criminalistiques de base

Une règle criminalistique doit contenir **exactement un** type d'événement criminalistique (par exemple, **Event Type == Unseen Command**). Les clauses facultatives suivantes utilisent les attributs de cet événement (par exemple, **Unseen Command - Parent Uptime**).

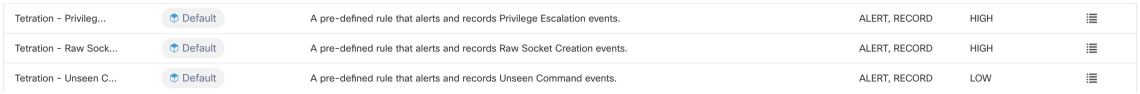
Vous trouverez ci-dessous un exemple d'utilisation du type d'événement **Unseen Command**. Pour obtenir d'autres exemples, consultez les règles par défaut et les règles MITRE.

EventType = Unseen Command et Unseen Command - Parent Uptime (microseconds) >= 60000000.

Règles Cisco Secure Workload par défaut

Les règles Cisco Secure Workload par défaut sont fournies pour aider les utilisateurs à élaborer des règles significatives dans leur environnement. Ces règles sont affichées dans la page de configuration criminalistique et elles ne sont pas modifiables. Les règles sont disponibles dans toutes les portées racine.

Figure 346: Règles par défaut



Les règles criminalistiques Cisco Secure Workload :

1. **Nom** Cisco Secure Workload - Escalade du privilège

   Clause EventType = Privilege Escalation and (**ProcessInfo - ExecPath** *doesn't contain* **sudo and ProcessInfo - ExecPath** *doesn't contain* **ping and Privilege Escalation Is** ⊨ **Type - Suid Binary**)

   Description. Cette règle signale les événements d'escalade de privilèges qui ne sont pas générés par les fichiers binaires setuid. Pour filtrer de manière fiable les fichiers binaires setuid, il est également possible de filtrer **sudo** et **ping** en fonction de « ProcessInfo - ExecPath ». Les utilisateurs Cisco Secure Workload peuvent également filtrer d'autres fichiers binaires setuid en définissant leurs propres règles.

2. **Name** Tetration - Commande non vue

   Clause EventType = Unseen Command and Unseen Command - Parent Uptime (microseconds) >= 60000000 or ProcessInfo - ExecPath *contains* **/bash or ProcessInfo - ExecPath** *contains* **/sh or ProcessInfo - ExecPath** *contains* **/ksh or Parent - ExecPath** *contains* **httpd or Parent - ExecPath** *contains* **apache or Parent - ExecPath** *contains* **nginx or Parent - ExecPath** *contains* **haproxy**

   Description. Cette règle signale les événements de commande non vues qui correspondent à l'un des critères suivants :

   a. Le processus parent est actif pendant plus de **60 000 000** de microsecondes.

   b. Le processus ExecPath contient un certain type d'interpréteur de commandes, par exemple **/bash**, **/sh** et **/ksh**.

   c. Le processus parent ExecPath contient un type d'application serveur, par exemple, **httpd**, **apache**, **nginx** et **haproxy**.

3. **Nom** Tetration - socket brut

   Clause EventType = Raw Socket Creation and (Raw Socket - ExecPath *doesn't contain* **ping and Raw Socket - ExecPath** *doesn't contain* **iptables and Raw Socket - ExecPath** *doesn't contain* **xtables-multi**)

   Description Cette règle signale les événements bruts de création de socket qui ne sont pas générés par **ping** et **iptables**. Les utilisateurs Cisco Secure Workload peuvent également filtrer d'autres fichiers binaires en définissant leurs propres règles.

4. **Name** Tetration - Anomalie de réseau avec commande non vue

   Clause EventType = Network Anomaly and Network Anomaly - Unseen Command Count > 3 and Network Anomaly - Non-seasonal Deviation > 0

   Description Cette règle signale les événements d'anomalie de réseau qui correspondent aux critères suivants :

a. Il y a plus de 3 événements de commande non vue sur la même charge de travail en 15 minutes.

b. L'Attributs de règles est supérieur à 0 (ce qui signifie également qu'il est supérieur ou égal à 6,0, car 6,0 est l'écart minimal signalé pour tous les événements d'anomalie de réseau).

5. **Name** Tetration - Commande anormale non vue

   Clause EventType = Unseen Command and Unseen Command - Anomaly - Score < 0.6

   Description Cette règle signale les événements de commande non vue dont la note d'anomalie est inférieure à 0,6. Cela signifie que seuls les événements fortement anormaux dont les commandes ne ressemblent pas aux commandes observées précédemment sont signalés. Le seuil de 0,6 est déterminé sur la base des expériences de Secure Workload concernant la similarité des commandes à différents seuils. Consultez Commande non vue pour une explication détaillée du résultat.

6. **Nom** Tetration : parent inhabituel de smss

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **smss.exe and (Follow Process - ParentExecPath** *doesn't contain* **smss.exe and Follow Process - ParentExecPath** *doesn't contain* **System)**

   Description Cette règle est spécifique à Windows. Cette règle alerte si smss.exe a un parent qui est différent d'une autre instance de smss.exe ou du processus système.

7. **Nom** Tetration - parent inhabituel de «wininit»

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **wininit.exe and Follow Process - ParentExecPath** *doesn't contain* **smss.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si wininit.exe a un parent différent de smss.exe.

8. **Nom** Tetration - parent inhabituel de RuntimeBroker

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **RuntimeBroker.exe and Follow Process - ParentExecPath** *doesn't contain* **svchost.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si RuntimeBroker.exe a un parent différent de svchost.exe.

9. **Nom** Tetration - parent inhabituel de services

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **services.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

   Description Cette règle est spécifique à Windows. Cette règle alerte si services.exe a un parent différent de winit.exe.

10. **Nom** Tetration - parent inhabituel de lsaio

    Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **lsaio.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

    Description Cette règle est spécifique à Windows. Cette règle alerte si lsaio.exe a un parent différent de « wininit.exe ».

11. **Nom** Tetration - Enfant inhabituel de lsass

Clause (EventType = Follow Process and ProcessInfo - ExecPath *doesn't contain* **efsui.exe and ProcessInfo - ExecPath** *doesn't contain* **werfault.exe**) **with ancestor Process Info - ExecPath** *contains* **lsass.exe**

Description Cette règle est spécifique à Windows. Cette règle alerte si lsass.exe a des descendants qui ne sont pas efsui.exe ou Werfault.exe.

Règles MITRE ATT&CK par défaut

Les règles par défaut de la fonction MITRE ATT&CK sont fournies pour envoyer des alertes techniques à partir du cadre de la fonction MITRE ATT&CK (https://attack.mitre.org/). Il y a 24 règles se rapportant au comportement malveillant et la plupart sont mises en correspondance à une technique MITRE particulière. La liste complète des règles se trouve ci-dessous.

1. **Nom** le comportement suspect de MS Office

   Clause (Event type = Follow Process and (Process Info - Exec Path doesn't contain **Windowssplwow64.exe) and (Process Info - Exec Path** *doesn't contain* **chrome.exe) and (Process Info - Exec Path** *doesn't contain* **msip.executionhost.exe) and (Process Info - Exec Path** *doesn't contain* **msip.executionhost32.exe) and (Process Info - Exec Path** *doesn't contain* **msosync.exe) and (Process Info - Exec Path** *doesn't contain* **ofcccaupdate.exe) with ancestor (Process Info - Exec Path** *contains* **winword.exe or Process Info -Exec Path** *contains* **excel.exe or Process Info -Exec Path contains powerpnt.exe)**

   Description Cette règle alerte et enregistre le fait que les processus Microsoft Office (WIN-WORD.exe/EXCEL.exe/POWERPNT.exe) créent des processus enfants. Sur la base de nos recherches, nous avons autorisé quelques processus enfants courants connus pour être créés par ces fichiers binaires MS Office, afin de réduire le nombre de faux positifs.

2. **Nom** T1015 – Fonctions d'accessibilité 1

   Clause Event type = Follow Process (Process Info - Exec Path *contains* **cmd.exe or Process Info -Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe**)

   Description Cette règle alerte et enregistre les cas où les fichiers binaires des fonctions d'accessibilité (clavier à l'écran, loupe, touches rémanentes, etc). sont utilisés de manière abusive et incitent à ouvrir cmd/powershell/cscript/wscript. L'appel des fichiers binaires d'accessibilité est contrôlé par les processus winlogon, atbroker ou utilman, selon l'endroit où ils sont appelés (à partir de l'écran de connexion ou après la connexion de l'utilisateur). Cette règle intercepte les processus enfants suspects (cmd.exe, powershell.exe, cscript.exe, wscript.exe) des processus d'accessibilité (winlogon.exe, utilman.exe et atbroker.exe). Utilisez-le avec **T1015 – Fonctionnalités d'accessibilité 2** pour détecter également les processus enfants supplémentaires de ces quatre processus enfants suspects**.

3. **Nom** T1015 – Fonctions d'accessibilité 2

   Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cmd.exe or Process Info - Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe))**

   Description Cette règle alerte et enregistre si l'un des exécutables des fonctionnalités d'accessibilité (clavier à l'écran, loupe, touches rémanentes, etc). est corrompu et incite à ouvrir

cmd.exe/powershell.exe/cscript.exe/wscript. exe. L'appel des fichiers binaires d'accessibilité est contrôlé par les processus winlogon, atbroker ou utilman, selon l'endroit où ils sont appelés (à partir de l'écran de connexion ou après la connexion de l'utilisateur). Cette règle capture les processus enfants suspects de ces processus (winlogon, utilman et atbroker). Il faut l'utiliser avec **T1015 – Fonctionnalités d'accessibilité 1** qui alerte les processus enfants suspects des fichiers binaires d'accessibilité.

4. **Nom** T1085 - runll32

   Clause (Event type = Follow Process and Process Info Exec Path *does not contain* **msiexec.exe and Process Info Exec Path** *does not contain* **WindowsSystem32SystemPropertiesRemote.exe with ancestor (Process Info - Exec Path** *contains* **rundll32.exe and Follow Process - Parent Exec Path** *does not contain* **msiexec.exe and not (Process Info -command string** *contains* **Windowssystem32shell32.dll or (Process Info -command string** *contains* **Windowssyswow64shell32.dll or (Process Info -command string** *contains* **WindowsSystem32migrationWinInetPlugin.dll))**

   Description Cette règle alerte et enregistre les cas où rundll32.exe crée des processus enfants. Ce fichier binaire peut être appelé pour exécuter des fichiers binaires/DLL quelconques ou utilisé par control.exe pour installer des éléments malveillants sur le panneau de configuration. Cependant, nous l'avons autorisé si msiexec.exe est le parent ou le descendant de runDLL32.exe. Nous avons également autorisé certaines des commandes courantes runDLL32 qui utilisent des DLL bien connues.

5. **Nom** T1118 – InstallUtil

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **hh.exe**

   Description Cette règle alerte et enregistre les cas où InstallUtil.exe crée des processus enfants.

6. **Nom** T1121 - Regsvcs/Remasm

   Clause Event type = Follow Process and (Process Info - Exec path *does not contain* **fondue.exe or Process Info - Exec path** *does not contain* **regasm.exe or Process Info - Exec path** *does not contain* **regsvr32.exe with ancestor (Process Info - Exec Path** *contains* **regasm.exe or Process Info - Exec Path** *contains* **regsvcs.exe)**

   Description Cette règle alerte et enregistre les cas où regsvcs.exe ou regasm.exe créent des processus enfants. Cependant, nous l'avons autorisée si fondue.exe/regasm.exe/regsvr32.exe est généré par regasm.exe ou regsvcs.exe afin de réduire le nombre de faux positifs.

7. **Nom** T1127 – Utilitaires pour développeurs de confiance – msbuild.exe

   Clause (Event type = Unseen Command with ancestor Process Info - Exec Path *contains* **MSBuild.exe) and (Process Info - Exec Path** *does not contain* **Tracker.exe) and (Process Info -Exec Path** *doesn't contain* **csc.exe) and (Process Info - Exec Path** *does not contain* **Microsoft Visual Studio) and (Process Info - Exec Path** *does not contain* **al.exe) and (Process Info - Exec Path** *does not contain* **lc.exe) and (Process Info - Exec Path** *does not contain* **dotnet.exe) and (Process Info - Exec Path** *does not contain* **cvtres.exe) and (Process Info - Exec Path** *does not contain* **conhost.exe) and not (Event type = Unseen Command with ancestor (Process Info - Exec Path** *contains* **Tracker.exe or Process Info - Exec Path** *contains* csc.exe or Process Info - Exec Path *contains* **Microsoft Visual Studio or Process Info - Exec Path** *contains* **al.exe or Process Info - Exec Path** *contains* **lc.exe or Process Info - Exec Path** *contains* **dotnet.exe or Process Info - Exec Path** *contains* **cvtres.exe))**

   Description Cette règle alerte et enregistre les cas où msbuild.exe crée des processus enfants qui n'appartiennent pas à une liste d'autorisation des processus enfants qu'il crée habituellement. Cette règle est actuellement basée sur la commande non vue, par opposition à Suivre le processus, car l'option Suivre le processus ne prend pas encore en charge l'autorisation des sous-arborescences de processus.

La règle actuelle autorise les processus suivants et leurs descendants : Tracker.exe, csc.exe, tout processus du chemin « Microsoft Visual Studio », al.exe, lc.exe, dotnet.exe et cvtres.exe. La règle autorise également conhost.exe. Ces processus peuvent être observés lors de l'utilisation normale de MSBuild.exe (par exemple, lors de la compilation d'un projet à l'aide de Visual Studio). Tous les autres descendants (comportement non habituel) de MSBuild.exe font l'objet d'alertes.

8. **Nom** T1127 – Utilitaires pour développeurs de confiance – rcsi.exe

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **rcsi.exe**

   Description Cette règle alerte et enregistre les cas où recsi.exe crée des processus enfants.

9. **Nom** T1127 – Utilitaires pour développeurs de confiance – tracker.exe

   Clause (Event type = Unseen Command with_ancestor Process Info - Exec Path *contains* **tracker.exe) and not (Event type = Unseen Command with_ancestor Process Info - Exec Path** *contains* **MSBuild.exe)**

   Description Cette règle alerte et enregistre les cas où tracker.exe crée des processus enfants et tracker lui-même n'est pas un descendant de MSBuild.exe. Ainsi, les appels légitimes du tracker via Visual Studio sont approuvés, mais les autres appels font l'objet d'alertes. L'une des limites des règles Tracker.exe et MSBuild.exe précédentes est que si un attaquant utilise la technique MSBuild pour créer Tracker, puis fait en sorte que Tracker crée un enfant malveillant, il ne sera pas alerté par l'une ou l'autre des règles puisque Tracker ayant MSBuild comme ancêtre est considéré comme légitime.

10. **Nom** T1128 – DLL de l'assistant Netsh

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **netsh.exe**

    Description Cette règle alerte et enregistre les cas où netsh.exe crée des processus enfants.

11. **Nom** T1136 - Créer un compte

    Clause Event type = User Account

    Description Cette règle alerte et enregistre la création d'un nouvel utilisateur.

12. **Nom** T1138 - Calage des applications

    Clause Event type = Follow Process Info - Exec Path *contains* **sdbinst.exe**

    Description Cette règle alerte et enregistre si sdbinst.exe est appelé.

13. **Name** T1180 - Économiseur d'écran

    Clause Event type = Follow Process AND with ancestor Process Info - Exec Path *contains* **.scr**

    Description Cette règle alerte et enregistre la création d'un processus avec la mention « .scr » dans le chemin d'exécution.

14. **Nom** T1191 – CMSTP

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **cmstp.exe**

    Description Cette règle alerte et enregistre les cas où cmstp.exe crée des processus enfants.

15. **Nom** T1202 – Exécution de commande indirecte – forfiles.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **forfiles.exe**

    Description Cette règle alerte et enregistre les cas où forfiles.exe crée des processus enfants.

16. **Nom** T1202 – Exécution de commande indirecte – pcalua.exe

Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **pcalua.exe**

Description Cette règle alerte et enregistre les cas où pcalua.exe crée des processus enfants.

17. **Nom** T1216 – Exécution de serveur mandataire de script signé – pubprn.vbs

    Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and Process Info - Command String** *contains* **.vbs and Process Info - Command String** *contains* **script)**

    Description Cette règle alerte et enregistre les cas où un script vbs est exécuté à l'aide de wscript.exe ou cscript.exe pour créer un nouveau processus, avec un paramètre « script ». Cette technique pourrait être utilisée par un attaquant pour exécuter pubprn.vbs avec un paramètre de script pointant vers un fichier sct malveillant, qui aurait alors pour but l'exécution du code.

18. **Nom** T1218 – Exécution du serveur mandataire binaire signé - msiexec.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **rcsi.exe**

    Description Cette règle alerte et enregistre les cas où msiexec.exe crée des processus enfants.

19. **Nom** T1218 – Exécution serveur mandataire binaire signé - odbcconf.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **odbcconf.exe**

    Description Cette règle alerte et enregistre les cas où odbcconf.exe crée des processus enfants.

20. **Nom** T1218 – Exécution du serveur mandataire binaire signé - Register-CimProvider

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **Register-CimProvider.exe**

    Description Cette règle alerte et enregistre les cas où Register-CimProvider.exe crée des processus enfants.

21. **Nom** T1220 – Traitement de script XSL – msxsl.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **msxsl.exe**

    Description Cette règle alerte et enregistre le cas où msxsl.exe crée des processus enfants.

22. **Nom** T1220 - Traitement de script XSL - wmic

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **wmic.exe and Process Info - Command String** *contains* **.xsl**)

    Description Cette règle alerte et enregistre les cas où un script xsl est utilisé par wmic. Cela peut être utilisé pour lancer des fichiers binaires quelconques.

23. **Nom** T1223 – Fichiers HTML compilés

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **hh.exe**

    Description Cette règle alerte et enregistre les cas où hh.exe crée des processus enfants.

24. **Nom** T1003 – Vidage des informations d'authentification – Lsass

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **procdump.exe and Process Info - Command String** *contains* **lsass**

    Description Cette règle alerte et enregistre les cas où processdump.exe est utilisé pour vider la mémoire des processus lsass.

25. **Nom** T1140 – Désobscurcissement/décodage des fichiers ou des renseignements

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **certutil.exe and (Process Info - Command String** *matches* **.*encode\s.* or Process Info - Command String** *matches* **.*decode\s.***

    Description Cette règle alerte et enregistre les cas où certutil.exe est utilisé pour coder ou décoder un fichier. Cette technique est souvent utilisée par les attaquants pour décoder leur charge utile codée sur l'ordinateur victime.

26. **Name** T1076 - Protocole de bureau à distance (Remote Desktop Protocol)

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **tscon.exe**

    Description Cette règle alerte et enregistre les cas où tscon.exe est exécuté. Les attaquants peuvent utiliser tscon.exe pour détourner des sessions RDP existantes.

27. **Nom** T1197 – Tâches BITS – Powershell

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **powershell.exe and Process Info - Command String** *contains* **Start-BitsTransfer**

    Description Cette règle alerte et enregistre les cas où powershell.exe est utilisé pour exécuter le cmdlet Start-BitsTransfer pour copier ou déplacer des fichiers.

28. **Nom** T1170 – MSHTA

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **mshta.exe**

    Description Cette règle alerte et enregistre les cas où mshta.exe est utilisé pour exécuter des scripts HTA malveillants qui engendrent des processus enfants.

29. **Nom** T1158 - Fichiers et répertoires masqués

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **attrib.exe and Process Info - Command String** *contains* **+h)**

    Description Cette règle alerte et enregistre les cas où attib.exe est utilisé pour définir un fichier/répertoire comme masqué.

30. **Name** T1114 - Collecte des courriels

    Clause Event type = Follow Process (Process Info - Command String *matches* **.*.(ost|pst)(\s|"|').* or Process Info - Command String** *matches* **.*.(ost|pst)$) Process Info - Exec Path** *doesn't contain* **outlook.exe**

    Description Cette règle alerte et enregistre les accès aux fichiers de courriel (.ost et .pst) à partir de tout autre processus qu'outlook.exe.

31. **Nom** T1070 – Retrait de l'indicateur sur l'hôte - Journal des événements

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **wevtutil.exe and Process Info - Command String** *matches* **.*\s(cl|clear-log)\s.***

    Description Cette règle alerte et enregistre les cas où wevtutil.exe est utilisé pour effacer les journaux des événements.

32. **Nom** T1070 – Retrait de l'indicateur sur l'hôte – USN

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **fsutil.exe and Process Info - Command String** *matches* **.*\susn\s.* and Process Info - Command String** *matches* **.*\sdeletejournal.***

Description Cette règle alerte et enregistre les cas où fsutil.exe est utilisé pour supprimer des journaux USN.

33. **Nom** T1053 - Tâche planifiée

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **schtasks.exe and Process Info - Command String** *contains* **create**

    Description Cette règle alerte et enregistre les cas où SCHTASK.exe est utilisé pour créer des tâches planifiées.

34. **Nom** T1003 - Vidage des informations d'authentification - Vaultcmd

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **vaultcmd.exe and Process Info - Command String** *matches* **.*\list.***

    Description Cette règle alerte et enregistre les cas où vaultcmd.exe est utilisé pour accéder au coffre-fort des informations d'authentification Windows.

35. **Nom** T1003 – Vidage des informations d'authentification - Registre

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **reg.exe and ((Process Info - Command String** *contains* **save or Process Info - Command String** *contains* **export) and (Process Info - Command String** *contains* **hklm or Process Info - Command String** *contains* **hkey_local_machine) and (Process Info - Command String** *contains* **sam or Process Info - Command String** *contains* **security or Process Info - Command String** *contains* **system))**

    Description Cette règle alerte et enregistre, les cas où reg.exe est utilisé, pour le vidage de certains éléments du registre.

36. **Nom** T1201 - Découverte de la politique en matière de mots de passe 1

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **change and Process Info - Command String** *contains* **-l**

    Description Cette règle alerte et enregistre les cas où l'utilitaire de modification est utilisé pour répertorier la politique de mot de passe (politique d'âge du mot de passe) sur un ordinateur Linux.

37. **Nom** T1081 – Informations d'authentification dans les fichiers – Linux

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **cat or Process Info - Exec Path** *contains* **grep) and (Process Info - Command String** *contains* **.bash_history or Process Info - Command String** *contains* **.password or Process Info - Command String** *contains* **.passwd)**

    Description Cette règle alerte et enregistre toute tentative de recherche de mots de passe stockés dans les fichiers sur un ordinateur Linux.

38. **Nom** T1081 - Informations d'authentification dans les fichiers - Windows

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **findstr.exe and Process Info - Command String** *contains* **password**

    Description Cette règle alerte et enregistre les tentatives de recherche de mots de passe stockés dans les fichiers sur un ordinateur Windows.

39. **Nom** T1089 – Désactivation des outils de sécurité

    Clause Event type = Follow Process and ((Process Info - Exec Path *contains* **fltmc.exe and Process Info - Command String** *contains* **unload sysmon) or (Process Info - Exec Path** *contains* **sysmon.exe and Process Info - Command String** *contains* **/u))**

Description Cette règle alerte et enregistre les tentatives de déchargement du pilote sysmon à l'aide de fltmc.exe ou de sysmon.exe

Profils criminalistiques

Ajouter un profil

Cette section explique comment ajouter de nouveaux profils criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

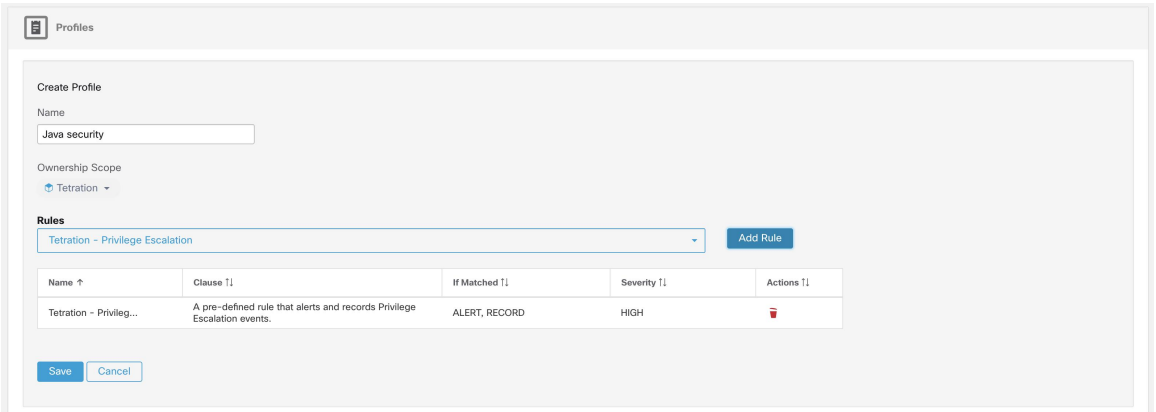
Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Cliquez sur **Create Profile** (Créer un profil)

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Nom : saisissez un nom pour le profil. Le nom ne peut pas être vide
Portée de la propriété	Saisissez une portée de propriété pour ce profil.
Règles	Ajoutez des règles à ce profil.

Figure 347: Créer un profil



Étape 4 Cliquez sur **Save** (enregistrer).

Modifier un profil

Cette section explique comment un utilisateur modifie des profils criminalistiques.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Repérez le profil que vous souhaitez modifier et cliquez sur l'icône en forme de **crayon** dans la colonne de droite.

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Mettez à jour le nom du profil. Le nom ne peut pas être vide
Portée de la propriété	Mettez à jour une portée de propriété pour ce profil.
Règles	Ajouter ou supprimer des règles de ce profil.

Étape 4 Cliquez sur **Save** (enregistrer).

Dupliquer un profil

Cette section explique comment un utilisateur clone les profils criminalistiques.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Defend (Défendre)** > **Forensic Rules (Règles criminalistiques)** .

Étape 2 Recherchez le profil que vous souhaitez cloner et cliquez sur l'icône de **clonage** dans la colonne de droite.

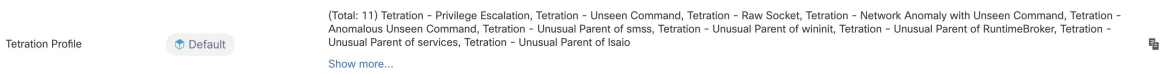
Étape 3 Saisissez le nom du profil cloné.

Étape 4 Cliquez sur **Save** (enregistrer).

Profil par défaut – Profil Cisco Secure Workload

Le profil Cisco Secure Workload contient 11 règles criminalistiques par défaut et peut être ajouté aux intents. Il n'est pas modifiable par l'utilisateur, mais il peut être cloné. Le profil criminalistique par défaut cloné est modifiable.

Figure 348: Profils par défaut



Profil par défaut - Profil MITRE ATT&CK

Le profil MITRE ATT&CK contient 39 règles MITRE ATT&CK et peut être ajouté aux intents. Il n'est pas modifiable par l'utilisateur, mais il peut être cloné. Le profil cloné est modifiable. Le profil MITRE ATT&CK comprend les règles suivantes :

1. Comportement suspect de MS Office
2. T1015 - Fonctionnalités d'accessibilité 1
3. T1015 - Fonctionnalités d'accessibilité 2
4. T1085 - runDLL32
5. T1118 - InstallUtil
6. T1121 - Regsvcs/Regasm
7. T1127 – Utilitaires pour développeurs de confiance – msbuild.exe
8. T1127 – Utilitaires pour développeurs de confiance – rcsi.exe
9. T1127 – Utilitaires pour développeurs de confiance – tracker.exe
10. T1128 – DLL de l'assistant Netsh
11. T1136 - Créer un compte
12. T1138 - Calage d'application
13. T1180 - Économiseur d'écran
14. T1191 - CMSTP
15. T1202 - Exécution indirecte de commandes - forfiles.exe
16. T1202 - Exécution indirecte de commandes - pcalua.exe
17. T1216 - Exécution de script de serveur mandataire signé - publicationprn.vbs
18. T1218 - Exécution serveur mandataire binaire signé - msiexec.exe
19. T1218 - Exécution serveur mandataire binaire signé - odbcconf.exe
20. T1218 - Exécution serveur mandataire binaire signé - Register-CimProvider
21. T1220 – Traitement des scripts XSL - msxsl.exe
22. T1220 – Traitement des scripts XSL – wmic
23. T1223 - Fichiers HTML compilés
24. T1003 - Vidage des informations d'authentification - Lsass
25. T1140 - Désobscurcissement/décodage de fichiers ou de renseignements
26. T1076 - Protocole de bureau à distance

27. T1197 - Opérations BITS – Powershell
28. T1170 – MSHTA
29. T1158 - Fichiers et répertoires masqués
30. T1114 - Collecte des courriels
31. T1070 – Retrait d'indicateur sur l'hôte - Journal des événements
32. T1070 – Retrait d'indicateur sur l'hôte – USN
33. T1053 - Tâche planifiée
34. T1003 - Vidage des informations d'authentification - Vaultcmd
35. T1003 - Vidage des informations d'authentification - Registre
36. T1201 - Découverte de la politique 1
37. T1081 - Renseignements d'authentification dans les fichiers - Linux
38. T1081 - Renseignements d'authentification dans des fichiers - Windows
39. T1089 - Désactivation des outils de sécurité

Journal des modifications : Criminalistique

Les **administrateurs du site** et les utilisateurs qui ont la capacité `SCOPE_OWNER` (PROPRIÉTAIRE DE PORTÉE) sur la portée racine peuvent afficher les journaux des modifications pour chaque règle, profil et intent criminalistique en cliquant sur l'icône, comme illustré ci-dessous.

Figure 349: Journal des modifications

Ces utilisateurs peuvent également afficher une liste des règles, des profils et des intents supprimés en cliquant sur le lien **View Deleted Rules/Profiles/Intents** (Afficher les règles, les profils et les intents supprimés) sous le tableau correspondant.

Pour en savoir plus sur le **journal des modifications**, consultez le Journal des modifications. Les propriétaires de la portée racine peuvent uniquement afficher les entrées du journal des modifications pour les entités appartenant à leur portée.

Visualisation criminalistique

Accès à la page Criminalistique

Cette section explique comment accéder à la page criminalistique.

Avant de commencer

Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Cliquez sur le lien **Security** (sécurité) dans le panneau de gauche.

Étape 2 Cliquez sur l'élément **criminalistique**. La page Criminalistique s'affiche.

Figure 350: Criminalistique de sécurité

Navigation parmi les événements criminalistiques

Cette section explique comment parcourir les événements criminalistiques correspondants.

Avant de commencer

Vous devez vous connecter en tant **qu'administrateur de site**, **service d'assistance à la clientèle** ou **propriétaire de la portée** dans le système et accéder à la page Criminalistique.

Procedure

Étape 1 Choisissez une plage spécifique dans le **sélecteur de plage temporelle** en haut de la page.

Étape 2 Sélectionnez **Severity** (gravité).

Étape 3 Dans **Filters**(filtres), saisissez les filtres des événements criminalistiques correspondants et cliquez sur **Filter Forensic Events**(filtrer les événements criminalistiques).

Étape 4 Le tableau des événements criminalistiques correspondants est mis à jour en fonction de la plage temporelle, de la gravité et des filtres sélectionnés.

Note Les événements criminalistiques sont visibles au niveau de la portée racine et ne le seront pas si l'on passe à des portées inférieures/enfants.

Inspection d'un événement criminalistique

Cette section explique comment inspecter les événements criminalistiques.

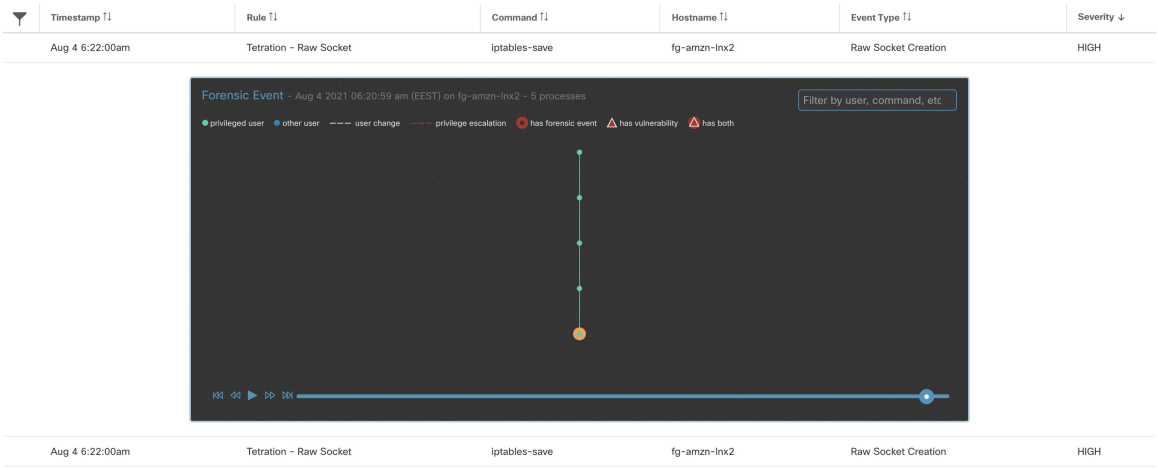
Avant de commencer

Vous devez vous connecter en tant **qu'administrateur de site**, **de service d'assistance à la clientèle** ou de **propriétaire de portée (portée racine)** au système.

Procedure

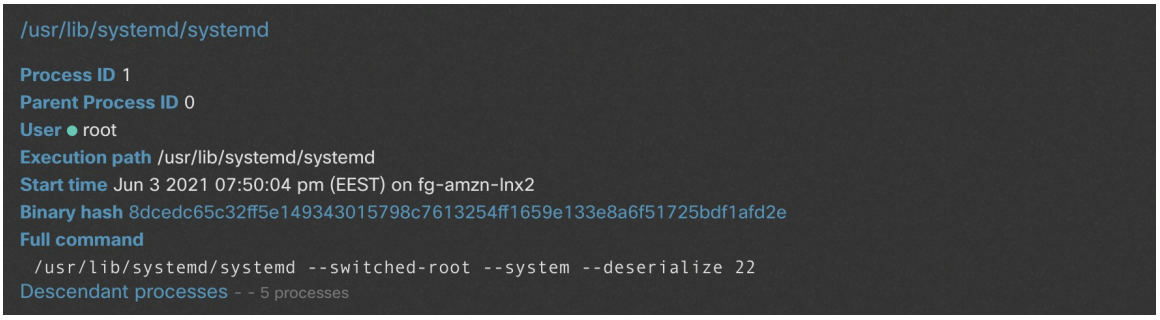
Étape 1 Cliquez sur l'événement à inspecter. Le volet **Détails du processus** s'affiche.

Figure 351: Tableau des événements criminalistiques



Étape 2 Dans l'arborescence, cliquez sur le processus à inspecter pour plus de détails.

Figure 352: Détails du processus criminalistique



Champs affichés dans les événements criminalistiques

Chaque événement criminalistique comporte plusieurs champs qui fournissent des données utiles. Il existe quelques champs communs à tous les différents types d'événements criminalistiques et quelques champs propres à un événement criminalistique particulier.

Vous trouverez ci-dessous une liste des champs qui font partie de l'interface utilisateur. Le premier tableau décrit les champs communs à tous les événements criminalistiques, suivi d'un tableau décrivant les informations sur le processus qui sont affichées avec chaque alerte, puis des tableaux contenant des champs uniques par événement criminalistique. Certains des champs peuvent être présents dans plusieurs tableaux, en raison de la façon dont les données sont stockées et exportées.

Champs communs

Champ	Description
Bin attr ctime	Modification de l'heure sous Linux / Création de l'heure du fichier binaire dans Windows
Bin attr hash	Condensé SHA256 du fichier binaire
Bin attr mtime	Heure modifiée du binaire
Bin attr name	Nom du fichier binaire sur le système de fichiers
Bin attr size	Taille du fichier binaire sur le système de fichiers
Bin exec path	Chemin complet du fichier binaire
Cmdline	Ligne de commande complète du processus à exécuter
Event time usec	Heure (en microsecondes) pendant laquelle cet événement est observé

Renseignements relatifs au processus

Champ	Description
Identifiant de processus	ID de processus du processus
ID du processus parent	ID de processus du parent du processus
Utilisateur	Utilisateur qui a exécuté le processus
Chemin d'exécution	Chemin complet du fichier binaire qui correspond au processus.
Heure de début	Heure à laquelle le processus a été lancé
Commande complète	Ligne de commande complète du processus à exécuter

Escalade de privilèges

Champ	Description
Parent cmdline	Ligne de commande complète du parent du processus
Parent exe	Chemin complet du parent du processus
Parent Uptime (microseconds)	Temps depuis l'exécution du parent du processus
Parent Username	Utilisateur qui a exécuté le parent du processus
Types bitmap suid binary	Indique si le bit SUID est défini sur binaire

Connexion de l'utilisateur

Champ	Description
Auth type password	Indique l'authentification par mot de passe
Auth type pubkey	Indique l'authentification par clé
Type login ssh	Indique qu'un utilisateur est connecté par SSH
Type login win batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Type login win cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Type login win interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Type login win network cleartext	Indique une connexion par SSH (type 8)
Type login win network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Type login win new cred	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Type login win remote interactive	Indique une connexion à distance (type 10, par exemple RDP)
Type login win service	Indique qu'un service a été démarré par SCM (type 5)
Type login win unlock	Indique que l'ordinateur a été déverrouillé (type 7)
Src IP	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Src Port	Port source à partir duquel l'événement de connexion a été généré
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Échec de connexion de l'utilisateur

Champ	Description
Auth type password	Indique l'authentification par mot de passe
Auth type pubkey	Indique l'authentification par clé
Type login ssh	Indique qu'un utilisateur est connecté par SSH

Champ	Description
Type login win batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Type login win cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Type login win interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Type login win network cleartext	Indique une connexion par SSH (type 8)
Type login win network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Type login win new cred	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Type login win remote interactive	Indique une connexion à distance (type 10, par exemple RDP)
Type login win service	Indique qu'un service a été démarré par SCM (type 5)
Type login win unlock	Indique que l'ordinateur a été déverrouillé (type 7)
Src IP	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Src Port	Port source à partir duquel l'événement de connexion a été généré
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Shellcode

Champ	Description
Sources de signaux bitmap cmd as sh no tty	Indique qu'un processus Shell n'est associé à aucun point terminal.
Powershell bitmap des sources de signal	Indique que le processus a chargé la dll powershell (System.Management.Automation)

Accès au fichier

Champ	Description
Fichier	Chemin complet du fichier consulté

Champ	Description
Lecture permanente	Indique que le fichier avait l'autorisation de lecture
Lecture écriture permanente	Indique que le fichier avait des autorisations de lecture et d'écriture
Écriture permanente	Indique que le fichier avait l'autorisation en écriture

Compte d'utilisateur

Champ	Description
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur qui a été créé
Ops acct add	Indique qu'un nouveau compte a été ajouté

Commande non vue

Champ	Description
Anomalie - Note	Note (0 à 1,0) indiquant la fréquence à laquelle la ligne de commande a été vue précédemment; une note plus basse signifie que la commande est plus anormale.
Anomalie - Similitude - Élevé	Vrai si le score d'anomalie est supérieur à 0,8 et est inférieur à 1
Anomalie - Similitude - Moyenne	Vrai si le score d'anomalie est supérieur à 0,6 et est inférieur ou égal à 0,8
Anomalie - Similitude - Faible	Vrai si le score d'anomalie est supérieur à 0 et est inférieur ou égal à 0,6
Anomalie - Similitude - Observé	Vrai si le score d'anomalie est de 1, c'est-à-dire que la même commande a déjà été vue
Anomalie - Similitude - Unique	Vrai si le score d'anomalie est de 0, c'est-à-dire que la commande n'a jamais été vue auparavant
Parent cmdline	Ligne de commande complète du processus parent
Parent exepath	Chemin binaire du processus parent
Temps de disponibilité du parent	Temps écoulé depuis l'exécution du processus parent
Parent username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Temps de disponibilité du capteur	Disponibilité du capteur

Bibliothèque non vue

Champ	Description
Chemin de la bibliothèque	Le chemin d'accès complet du fichier de bibliothèque qui n'était pas associé au processus auparavant

Création d'interface de connexion brute

Champ	Description
Chemin d'accès exe	Chemin complet du processus qui a créé le connecteur brut

Bibliothèque modifiée

Champ	Description
Le nom de la bibliothèque modifié	Le chemin d'accès complet de la bibliothèque qui a été modifiée

Canaux auxiliaires

Champ	Description
Fusion de bitmap des sources de signal	Indique l'utilisation de l'exploit « meltdown » (Fusion)

Suivre la connexion de l'utilisateur

Champ	Description
Nom d'utilisateur	Nom de l'utilisateur qui a exécuté le processus

Suivre le processus

Champ	Description
Parent cmdline	Ligne de commande complète du processus parent
Parent exepath	Chemin binaire du processus parent
Parent uptime usec	Temps écoulé depuis l'exécution du processus parent
Parent username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent

Champ	Description
Time since last changed usec	Temps écoulé entre l'heure de début du processus et son heure de changement de fichier binaire (mtime)
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur qui a exécuté le processus

Anomalie de réseau

Pour en apprendre davantage, consultez la page Règles de criminalistique pour les événements d'anomalie de réseau (détection des anomalies de réseau) pour obtenir la liste des attributs associés aux événements d'anomalies de réseau.

Analyse criminalistique : zones de recherche

Les tableaux ci-dessous décrivent les champs de recherche de la barre de recherche de la page Forensics Analysis (Analyse criminalistique).

Champs divers

Champ	Description
Nom de la règle criminalistique	Événements marqués par une règle criminalistique particulière
Nom d'hôte	Événements provenant d'un nom d'hôte particulier
ID du capteur	Événements provenant d'un capteur particulier
Gravité	Événements d'une gravité particulière

Termes de recherche dans les analyses criminalistiques

Champs communs

Ces champs sont communs à différents types d'événements. Ils ont le préfixe « Nom de l'événement – Événement ». Par exemple, « Binary Changed – Binary Attribute – CTime (epoch nanoseconds) »

Champ	Description
Binary Attribute - CTime (epoch nanoseconds)	Modification de l'heure sous Linux / Création de l'heure du fichier binaire dans Windows
Binary Attribute - Hash	Condensé SHA256 du fichier binaire

Champ	Description
Binary Attribute - MTime (epoch nanoseconds)	Heure modifiée du binaire
Binary Attribute - Filename	Nom du fichier binaire sur le système de fichiers
Binary Attribute - Size (bytes)	Taille du fichier binaire sur le système de fichiers
Event Binary Path	Chemin complet du fichier binaire
Ligne de commande	Ligne de commande complète du processus à exécuter

Fichier binaire modifié

Il n'y a aucun autre terme de recherche que ceux décrits dans le tableau « Champs communs ».

Accès au fichier

Les termes de recherche pour l'accès au fichier ont le préfixe « Accès au fichier – » par exemple « Accès au fichier – Nom de fichier ».

Champ	Description
Nom de fichier	Chemin complet du fichier consulté
Is = Permission - Read	Indique que le fichier avait l'autorisation de lecture
Is = Permission - ReadWrite	Indique que le fichier avait des autorisations de lecture et d'écriture
Is = Permission - Write	Indique que le fichier avait l'autorisation en écriture

Suivre le processus

Les termes de recherche de suivi de processus ont le préfixe « Follow Process – » (Suivez le processus) par exemple « Follow Process - Parent Command Lin ».

Champ	Description
Parent Command Line	Ligne de commande complète du processus parent
Parent Exec Path	Chemin binaire du processus parent
Parent Uptime (microseconds)	Temps écoulé depuis l'exécution du processus parent
Parent Username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Heure de début du processus depuis la dernière modification de fichier (microsecondes)	Temps qui s'écoule entre le début du processus et la dernière modification de fichier (correspondante)
Nom d'utilisateur	Noms d'utilisateur associés au processus suivi

Suivre la connexion de l'utilisateur

Les termes de recherche du suivi de la connexion de l'utilisateur ont le préfixe « Follow User Logon - » par exemple « Follow User Logon - Username » (suivre la connexion de l'utilisateur - nom d'utilisateur).

Champ	Description
Nom d'utilisateur	Nom d'utilisateur associé à un processus

Ldap

Les termes de recherche Ldap ont le préfixe « Ldap - », par exemple « Ldap - Department »

Champ	Description
Service	Service utilisateur AMS Ldap associé au nom d'utilisateur du processus (si disponible)
Description	Description d'utilisateur AMS Ldap associée au nom d'utilisateur du processus (si disponible)
Nom d'utilisateur	Nom d'utilisateur AMS Ldap associé au processus (si disponible)

Bibliothèque modifiée

Les termes de recherche Library Changed (modification de bibliothèque) ont le préfixe « Library Changed – » ou « Library Changed – Service »

Champ	Description
Nom de fichier Lib	Le chemin d'accès complet de la bibliothèque qui a été modifiée

Escalade de privilèges

Les termes de recherche d'escalade de privilèges sont précédés du préfixe « Privilege Escalation – », par exemple « Privilege Escalation - Parent Command line (ligne de commande parente) ».

Champ	Description
Parent Command Line	Ligne de commande complète du parent du processus
Parent Exec Path	Chemin complet du parent du processus
Parent Uptime (microseconds)	Temps depuis l'exécution du parent du processus
Parent Username	Utilisateur qui a exécuté le parent du processus
Type - Suid Binary	Indique si le bit SUID est défini sur binaire

Renseignements relatifs au processus

Les termes de recherche des informations de processus ont le préfixe « Process Info - », par exemple « Process Info - binaryHash ».

Champ	Description
Condensé binaire	Condensé du fichier binaire associé au processus
Chaîne de commande marquée d'un jeton	Ligne de commande marquée d'un jeton du processus
Chaîne de commande	Ligne de commande complète du processus
Chemin d'accès exécutable	Chemin complet du fichier binaire qui correspond au processus

Connecteur brut

Les termes de recherche du connecteur brut comportent le préfixe « Raw Socket - ». Par exemple, « Raw Socket - Exec Path »

Champ	Description
Chemin d'accès exécutable	Chemin complet du processus qui a créé le connecteur brut

Shellcode

Les termes de recherche de code Shell ont le préfixe « Shellcode - ». Par exemple, « Shellcode - Source - Non issue de la connexion »

Champ	Description
Source – Non issue de la connexion	Indique qu'un processus Shell n'est associé à aucun point terminal.
Source – Powershell	Indique que le processus a chargé la dll powershell (System.Management.Automation)

Canaux auxiliaires

Les termes de recherche des Canaux auxiliaires ont le préfixe « Shellcode - ». Par exemple, « Shellcode - Source - Fusion »

Champ	Description
Source - Fusion	Indique l'utilisation de l'exploit « meltdown » (Fusion)

Commande non vue

Les termes de recherche de commandes non vues sont précédés du préfixe « Unseen Command – » (Commande inconnue) – Anomalie – Similitude – Élevée).

Champ	Description
Anomalie - Note	Note (0 à 1,0) indiquant la fréquence à laquelle la ligne de commande a été vue précédemment; une note plus basse signifie que la commande est plus anormale.
Anomalie - Similitude - Élevé	Vrai si le score d'anomalie est supérieur à 0,8 et est inférieur à 1
Anomalie - Similitude - Moyenne	Vrai si le score d'anomalie est supérieur à 0,6 et est inférieur ou égal à 0,8
Anomalie - Similitude - Faible	Vrai si le score d'anomalie est supérieur à 0 et est inférieur ou égal à 0,6
Anomalie - Similitude - Observé	Vrai si le score d'anomalie est de 1, c'est-à-dire que la même commande a déjà été vue
Anomalie - Similitude - Unique	Vrai si le score d'anomalie est de 0, c'est-à-dire que la commande n'a jamais été vue auparavant
Parent Cmdline	Ligne de commande complète du processus parent
Parent Exepath	Chemin binaire du processus parent
Temps de disponibilité du parent	Temps écoulé depuis l'exécution du processus parent
Parent Username	Nom d'utilisateur de l'utilisateur qui a exécuté le processus parent
Temps de disponibilité du capteur	Disponibilité du capteur
Anomalie - Dernières commandes similaires	Cinq dernières commandes similaires à la commande de l'événement observées précédemment

Bibliothèque non vue

Les termes de recherche de bibliothèque non vue ont le préfixe « Unseen Library – » par exemple « Unseen Library – Lib Filename »

Champ	Description
Nom de fichier Lib	Le chemin d'accès complet du fichier de bibliothèque qui n'était pas associé au processus auparavant

Compte d'utilisateur

Les termes de recherche des comptes d'utilisateurs ont le préfixe « User Account – » par exemple « User Account – Account Name » (Nom du compte).

Champ	Description
Nom du compte	Nom d'utilisateur de l'utilisateur qui a été créé
Operation - Add Account	Indique qu'un nouveau compte a été ajouté

Connexion de l'utilisateur

Les termes de recherche de connexion d'utilisateur ont le préfixe « User Logon – » par exemple « User Logon - Auth Type - Password » (mot de passe).

Champ	Description
Auth Type - Password	Indique l'authentification par mot de passe
Auth type - Pubkey	Indique l'authentification par clé
Login Type - Login Via SSH	Indique qu'un utilisateur est connecté par SSH
Login Type - Windows Login Batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Login Type - Windows Login Cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Login Type - Windows Login Interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Login Type - Windows Network Cleartext	Indique une connexion par SSH (type 8)
Login Type - Windows Network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Login Type - Windows Login New Credential	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Login Type - Windows Login Remote Interactive	Indique une connexion à distance (type 10, par exemple RDP)
Login Type - Windows Login Service	Indique qu'un service a été démarré par SCM (type 5)
Login Type - Windows Login Unlock	Indique que l'ordinateur a été déverrouillé (type 7)
IP de la source	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Source Port (port source)	Port source à partir duquel l'événement de connexion a été généré

Champ	Description
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Échec de connexion de l'utilisateur

Les termes de la recherche User Logon Failed sont précédés du préfixe « User Logon Failed - ».Par exemple, « User Logon Failed - Auth Type - Password »

Champ	Description
Auth Type - Password	Indique l'authentification par mot de passe
Auth type - Pubkey	Indique l'authentification par clé
Login Type - Login Via SSH	Indique qu'un utilisateur est connecté par SSH
Login Type - Windows Login Batch	Indique une connexion Windows par lots (type 4, p. ex., schtasks)
Login Type - Windows Login Cached	Indique la connexion avec des informations d'authentification en cache (type 11, CachedIntetractive)
Login Type - Windows Login Interactive	Indique une connexion interactive (type 2, p. ex., RDP)
Login Type - Windows Network Cleartext	Indique une connexion par SSH (type 8)
Login Type - Windows Network	Indique une connexion au réseau (type 3, p. ex., Psexec)
Login Type - Windows Login New Credential	Indique l'utilisation de nouveaux identifiants (type 9, p. ex., commande Runas)
Login Type - Windows Login Remote Interactive	Indique une connexion à distance (type 10, par exemple RDP)
Login Type - Windows Login Service	Indique qu'un service a été démarré par SCM (type 5)
Login Type - Windows Login Unlock	Indique que l'ordinateur a été déverrouillé (type 7)
IP de la source	Adresse IP source à partir de laquelle l'événement de connexion a été généré
Source Port (port source)	Port source à partir duquel l'événement de connexion a été généré
Nom d'utilisateur	Nom d'utilisateur associé à l'événement de connexion

Alertes criminalistiques

Les événements criminalistiques peuvent être trouvés dans le système d'alerte Cisco Secure Workload si leurs règles de correspondance contiennent une action d' **alerte**.

Accès aux alertes criminalistiques

Cette section explique comment accéder aux alertes criminalistiques.

Avant de commencer

- Connectez-vous au système en tant **qu'administrateur de site**, **service d'assistance à la clientèle** ou **propriétaire de la portée**.
- Activez les alertes pour la source d'alerte **criminalistique**.

Procedure

Étape 1 Dans le volet de navigation, sélectionnez **Configure Alerts** (Configurer les alertes).

Étape 2 La page d'alertes s'affiche.

Vérification des détails de l'alerte

Avant de commencer

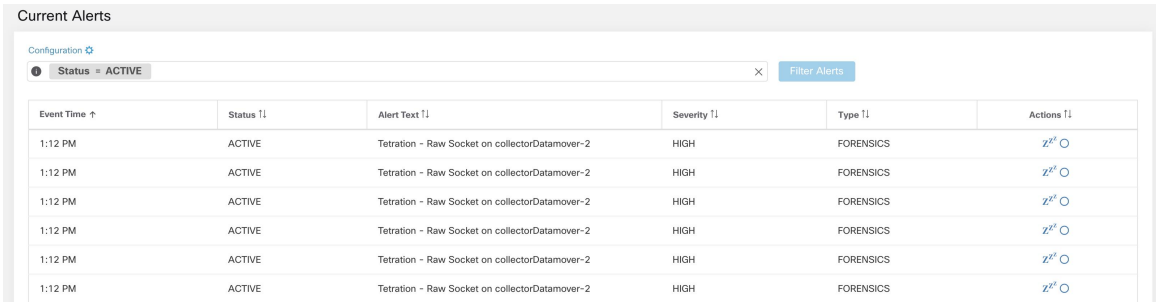
Vous devez vous connecter au système en tant **qu'administrateur de site**, de **service d'assistance à la clientèle** ou de **propriétaire de la portée**.

Procedure

Étape 1 Dans la page d'alertes, cliquez sur l'alerte à vérifier.

Étape 2 Cliquez sur profile/rule (Profil/Nom) pour afficher les détails de la règle ou du profil criminalistique correspondant. Si le profil/la règle correspondant(e) est mis(e) à jour après l'émission d'alertes, un indicateur d'avertissement s'affiche.

Figure 353: Page d'alerte criminalistique



En outre, vous pouvez répéter ou inclure/exclure une alerte. Reportez-vous à la section Alertes actuelles pour en savoir plus.

Intégration externe

Des alertes criminalistiques peuvent être envoyées à des outils de surveillance externes tels que syslog. L'alerte criminalistique est envoyée au format JSON. Les définitions des champs JSON sont indiquées dans la section « Champs affichés dans les événements criminalistiques » ci-dessus.

Vous trouverez ci-dessous un exemple de sortie JSON Kafka :


```
  {
    "severity": "HIGH",
    "tenant_id": 0,
    "alert_time": 1595573847156,
    "alert_text": "Tetration - Anomalous Unseen Command on collectorDatamover-1",
    "key_id":
"d89f926cddc7577553eb8954e492528433b2d08e:5efcfdf5497d4f474f1707c2:5efcfdf6497d4f474f1707d6:20196:CMD_NOT_SEEN",

    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='forensics', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/db10d21631eebefc3b8d3aeaba5a0b1b45f4259e85b591763d7eaee9161ca076",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "FORENSICS",
    "event_time": 1595573795135,
    "alert_details": "{\"Sensor
Id\":\"d89f926cddc7577553eb8954e492528433b2d08e\",\"Hostname\":\"collectorDatamover-1\",\"Process
 Id\":20196,\"scope_id\":\"5efcfdf5497d4f474f1707c2\",\"forensic\":{\"Unseen
Command\":\"true\",\"Unseen Command - Sensor Uptime (microseconds)\":\"34441125356\",\"Unseen
 Command - Parent Uptime (microseconds)\":\"35968418683\",\"Unseen Command - Parent
Username\":\"root\",\"Unseen Command - Parent Command Line\":\"svlogd -tt
/local/logs/tetration/efe/ \",\"Unseen Command - Parent Exec Path\":\"/sbin/svlogd\",\"Unseen
 Command - Anomaly - Score\":\"0\",\"Unseen Command - Anomaly - Similarity -
Unique\":\"true\",\"Process Info - Command String\":\"gzip \",\"Process Info - Exec
Path\":\"/bin/gzip\"},\"profile\":{\"id\":\"5efcfdf6497d4f474f1707e4\",\"name\":\"Tetration

Profile\",\"created_at\":1593683390,\"updated_at\":1593683390,\"root_app_scope_id\":\"5efcfdf5497d4f474f1707c2\"},\"rule\":{\"id\":\"5efcfdf6497d4f474f1707d6\",\"name\":\"Tetration
 - Anomalous Unseen
Command\",\"clause_chips\":\"[{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"event_type\\\",\\\"title\\\":\\\"Event

type\\\",\\\"type\\\":\\\"STRING\\\"},\\\"operator\\\":{\\\"label\\\":\\\"\\u003d\\\",\\\"type\\\":\\\"eq\\\"},\\\"displayValue\\\":\\\"Unseen
 Command\\\",\\\"value\\\":\\\"Unseen
Command\\\"},{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info__score\\\",\\\"title\\\":\\\"Unseen
```

```
 Command - Anomaly -
Sc\",\"ye\":\"NMR\"},\"pera\":{\"la\":\"\u02\",\"ye\":\"1\"},\"displayVa\":\"0.6\",\"va\":\"0.6\"}]","created_at":1595539498,"updated_at":1595539498,"root_app_scope_id":"5efcfdf5497d4f474f1707c2"}"

  }
```


La valeur dans alert_détails est elle-même une chaîne JSON échappée dont le contenu pour l'alerte ci-dessus est visible ci-dessous :


```
  {
    "Sensor Id": "d89f926cddc7577553eb8954e492528433b2d08e",
    "Hostname": "collectorDatamover-1",
    "Process Id": 20196,
    "scope_id": "5efcfdf5497d4f474f1707c2",
    "forensic": {
      "Unseen Command": "true",
      "Unseen Command - Sensor Uptime (microseconds)": "34441125356",
      "Unseen Command - Parent Uptime (microseconds)": "35968418683",
      "Unseen Command - Parent Username": "root",
      "Unseen Command - Parent Command Line": "svlogd -tt /local/logs/tetration/efe/ ",
      "Unseen Command - Parent Exec Path": "/sbin/svlogd",
      "Unseen Command - Anomaly - Score": "0",
      "Unseen Command - Anomaly - Similarity - Unique": "true",
      "Process Info - Command String": "gzip ",
      "Process Info - Exec Path": "/bin/gzip"
    },
    "profile": {
      "id": "5efcfdf6497d4f474f1707e4",
      "name": "Tetration Profile",
      "created_at": 1593638390,
      "updated_at": 1593638390,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    },
    "rule": {
      "id": "5efcfdf6497d4f474f1707d6",
      "name": "Tetration - Anomalous Unseen Command",
      "clause_chips":
"[{\"type\":\"filter\",\"facet\":{\"field\":\"event_type\",\"title\":\"Event
type\",\"type\":\"STRING\"},\"operator\":{\"label\":\"=\",\"type\":\"eq\"},\"displayValue\":\"Unseen
 Command\",\"value\":\"Unseen
Command\"},{\"type\":\"filter\",\"facet\":{\"field\":\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info__score\",\"title\":\"Unseen
 Command - Anomaly -
Score\",\"type\":\"NUMBER\"},\"operator\":{\"label\":\"<\",\"type\":\"lt\"},\"displayValue\":\"0.6\",\"value\":\"0.6\"}]",

      "created_at": 1593638390,
      "updated_at": 1595539498,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    }
  }
```


Les détails des événements criminalistiques sont inclus dans le champ criminalistique. Pour obtenir la liste des attributs des événements criminalistiques, consultez Champs affichés dans les événements criminalistiques. Ces attributs sont également affichés dans les détails de l'alerte dans l'interface utilisateur.

Note de criminalistique

Où voir la note criminalistique

Tableau de bord de sécurité

Figure 354: Section de la note criminalistique dans le tableau de bord de la sécurité

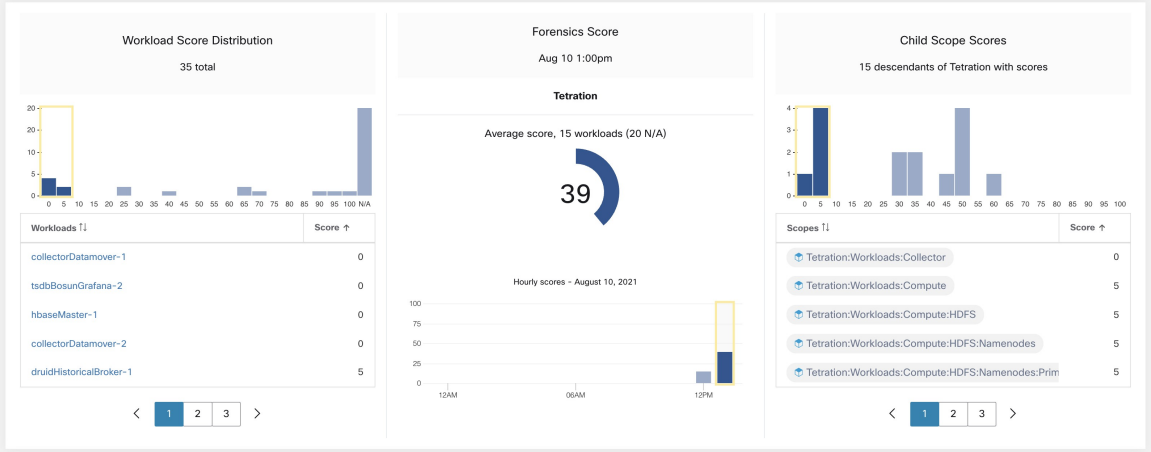
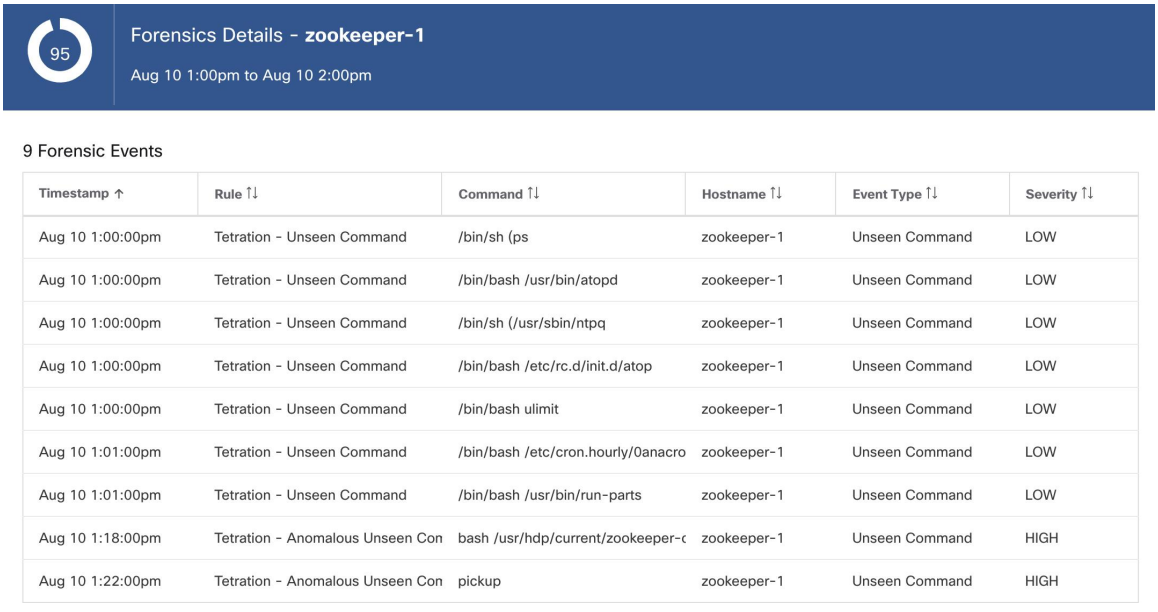


Figure 355: Section des détails de la note criminalistique dans le tableau de bord de la sécurité



9 Forensic Events

Timestamp	Rule	Command	Hostname	Event Type	Severity
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (ps	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/atopd	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (/usr/sbin/ntpq	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /etc/rc.d/init.d/atop	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash ulimit	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /etc/cron.hourly/0anacro	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/run-parts	zookeeper-1	Unseen Command	LOW
Aug 10 1:18:00pm	Tetration - Anomalous Unseen Con	bash /usr/hdp/current/zookeeper-c	zookeeper-1	Unseen Command	HIGH
Aug 10 1:22:00pm	Tetration - Anomalous Unseen Con	pickup	zookeeper-1	Unseen Command	HIGH

Comment la note de criminalistique est-elle calculée?

Pour chaque charge de travail, nous calculons une note criminalistique. La note criminalistique d'une charge de travail est calculée à partir des événements criminalistiques observés sur cette charge de travail en fonction

des profils activés pour cette portée. Une note de 100 signifie qu'aucun événement criminalistique n'a été observé par les règles configurées dans les profils activés, et une note de 0 signifie qu'un événement criminalistique a été détecté qui nécessite une action immédiate. La note criminalistique d'une portée est la note moyenne de charge de travail dans cette portée. La note criminalistique pour une heure donnée est le minimum de tous les résultats de cette heure.

- Un événement criminalistique ayant le niveau de gravité REQUIRES IMMEDIATE ACTION (NÉCESSITE UNE ACTION IMMÉDIATE) réduit la note de l'ensemble de la portée à zéro.
- Un événement criminalistique avec le niveau de gravité CRITICAL (CRITIQUE) réduit la note de la charge de travail avec une pondération de 10.
- Un événement criminalistique avec le niveau de gravité HIGH (ÉLEVÉ) réduit la note de la charge de travail avec une pondération de 5.
- Un événement criminalistique avec la gravité MEDIUM (MOYENNE) réduit la note de la charge de travail avec une pondération de 3.
- Un événement criminalistique ayant la gravité LOW (FAIBLE) ne contribue pas à la note criminalistique. Cela est recommandé pour les nouvelles règles lorsque la qualité du signal est toujours en cours d'optimisation et est susceptible d'être bruitée.

Par exemple, une charge de travail comporte 3 événements criminalistiques qui correspondent respectivement à 2 règles de gravité *CRITIQUE* , 1 règle de gravité *ÉLEVÉE* et 1 règle de gravité *FAIBLE*. La note criminalistique pour cette charge de travail est : 100 – 1 * 10 – 1 * 5 – 1 * 0 = 85.

Les notes criminalistiques sont S.O. pour les charges de travail dans lesquelles la fonction criminalistique n'est pas activée.

Comment améliorer la note criminalistique

Vous pouvez régler votre note criminalistique en ajustant les règles criminalistiques activées. En créant des règles moins parasitées, vous obtiendrez une note plus précise. La prise en compte et la prévention d'événements criminalistiques légitimes (les événements qui sont la preuve d'une intrusion ou d'une autre activité malveillante) sont un autre bon moyen d'améliorer votre score criminalistique.

Mises en garde

- Les détails de la note criminalistique affichent tous les événements criminalistiques au cours de cette heure. Cela signifie que les détails de la note criminalistique peuvent afficher des événements légaux autres que ceux utilisés pour le calcul de cette dernière.
- La note criminalistique est actuellement disponible pour les capteurs de visibilité approfondie et d'application.

Détection des anomalies de réseau basée sur le PCR

La fonction d'anomalie de réseau détecte des quantités anormalement importantes de données qui entrent ou sortent des charges de travail selon le concept de rapport producteur-consommateur (PCR). Le PCR est défini comme suit :

```
Egress app byte count - Ingress app byte count
  PCR = ------------------------------------------
        Egress app byte count + Ingress app byte count
```

La valeur de PCR se trouve dans la plage [-1.0, 1.0], où :

- PCR = 1.0 signifie que la charge de travail envoie uniquement des données.
- PCR = -1,0 signifie que la charge de travail reçoit uniquement des données.
- PCR = 0.0 signifie que la charge de travail a équilibré les quantités de données entrantes et sortantes.

Comme pour les autres fonctionnalités criminalistiques, vous pouvez utiliser la configuration basée sur les intents pour configurer les événements d'anomalies de réseau que vous souhaitez enregistrer ou sur lesquels vous souhaiter alerter. Les événements d'anomalies de réseau détectées des charges de travail sont exportés toutes les 5 minutes et comparés aux règles configurées 5 minutes plus tard. Par conséquent, les nouveaux événements d'anomalie de réseau ne sont observés sur l'interface utilisateur que toutes les 5 minutes avec un retard pouvant aller jusqu'à 10 minutes à partir du moment de survenance de l'événement.

Note Dans les versions 3.2 et 3.1 du logiciel Cisco Secure Workload, la détection des anomalies de réseau était appelée détection de fuites de données.

Règles de criminalistique pour les événements d'anomalie de réseau

Consultez Configuration criminalistique sur la façon d'ajouter des règles criminalistiques.

Attributs de règles

Cette section explique les détails des attributs pour définir une règle liée à une anomalie de réseau. La règle d'anomalie de réseau la plus simple est :

```
Event Type = Network Anomaly
```

Autres attributs dans l'événement Anomalie de réseau pour affiner les règles pour vos centres de données :

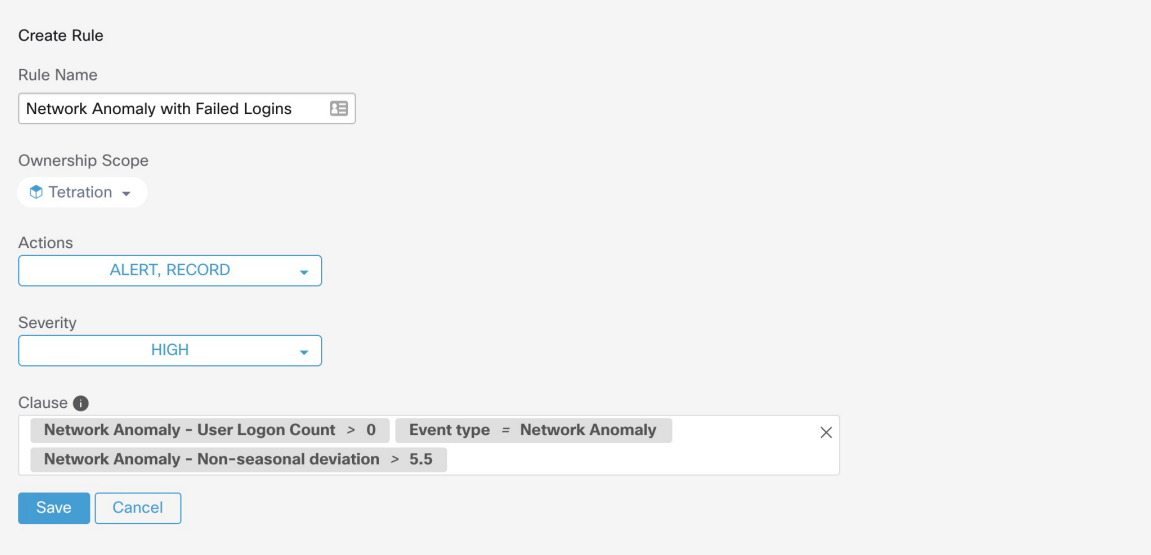
Table 32: Attributs de règle dans l'événement Anomalie de réseau

Attribut	Description
Nom de l'hôte	Le nom d'hôte du travail qui émet cet événement.
Horodatage (origine, millisecondes)	Horodatage (en millisecondes) de l'événement.
Écart PCR	L'écart du PCR (Rapport Fournisseur-Consommateur) par rapport à la moyenne au moment de l'événement en tant que multiple de l'écart type historique.
Écart non saisonnier	Il s'agit de l'écart PCR après suppression du modèle de saisonnalité (par exemple, par tâches cron). La valeur de l'écart non saisonnier est toujours supérieure ou égale à 6.
PCR	Le rapport fournisseurs-consommateurs.

Attribut	Description
EIR	Le rapport d'entrée de sortie, qui est le rapport entre le nombre total d'octets d'application de sortie et le nombre d'octets d'application d'entrée.
Nombre d'octets d'application de sortie	Le nombre d’octets d’application de sortie, qui correspond au nombre total d’octets du contenu des paquets (à l’exclusion des en-têtes) sortant de la charge de travail.
Nombre d'octets d'application d'entrée	Le nombre d'octets d'application entrants, qui est le nombre total d'octets du contenu des paquets (à l'exclusion des en-têtes) circulant dans la charge de travail.
Protocole	Le protocole pour lequel la série chronologique du PCR est calculée. Actuellement, les protocoles pris en charge sont TCP, UDP et Aggregate. La fonction Aggregate PCR est calculée en fonction de la somme totale des nombres d’octets TCP, UDP et ICMP.
Nombre de connexion d’utilisateurs	Le nombre d'événements de connexion d’utilisateur sur la charge de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements de connexion de l'utilisateur, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements de connexion de l'utilisateur, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.
Nombre d'échecs de connexion de l’utilisateur	Le nombre d’échecs de connexion des utilisateurs sur le charges de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements d'échec de la connexion de l'utilisateur, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements d'échec de connexion de l'utilisateur, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.
Nombre de commandes non vues	Le nombre d’événements de commande non vues sur la charge de travail au cours des 15 dernières minutes environ. Il s'agit du nombre d'événements de commandes non vues, qu'il existe ou non des règles correspondantes. Pour connaître les détails des événements de commandes non vues, vous devez définir des règles pour enregistrer les événements pour les charges de travail qui vous intéressent et les afficher sur la page Analyse criminalistique.

Attribut	Description
Date, heure (UTC) - année	L'année de l'événement.
Date, heure (UTC) - Mois	Le mois de l'heure de l'événement (1, 2, etc. . .).
Date, heure (UTC) - Jour	Le jour du mois de l'heure de l'événement (1, 2, etc. . .).
Date, heure (UTC) - Heure	L'heure du jour de l'événement (1, 2, . . . , 24).
Date, heure (UTC) - Minutes	Minute d'une heure de l'événement (1, 2,. . . , 60).
Date, heure (UTC) - Seconde	La seconde de la minute de l'heure de l'événement (1, 2,. . . , 60).
Date, heure (UTC) - Jour de la semaine	Le jour de la semaine correspondant à l'heure de l'événement (0 à 7 pour lundi au dimanche).

Figure 356: Définition de règles criminalistiques pour les événements d'anomalie de réseau



Vous trouverez ci-dessous des exemples de règles :

Listing 7.10.1.1.1 : Détecte les anomalies de réseau pour UDP uniquement.

```
Event Type = Network Anomaly AND Network Anomaly Is = Protocol - UDP
```

Listing 7.10.1.1.2 : Détecte les écarts importants après la suppression du modèle saisonnier (s'il est détecté), avec un seuil sur le nombre d'octets d'application de sortie pour un sous-ensemble de charges de travail dont les noms contiennent *sensibleDataServer*.

```
Event Type = Network Anomaly AND Network Anomaly - Non-seasonal Deviation > 10.0)
AND Network Anomaly - Egress App Byte Count > 1000000
AND Network Anomaly - Host Name CONTAINS sensitiveDataServer
```

Listing 7.10.1.1.3 : Détecte les événements d'anomalie de réseau sur les charges de travail avec des événements de commande non vues, à l'exception des événements d'anomalie de réseau qui se produisent de 7 h 30 UTC à 7 h 35 UTC tous les jours.

```
    Event Type = Network Anomaly AND Network Anomaly - Unseen Command Count > 0
    AND ( Network Anomaly - Date Time (UTC) - Hour != 7
    OR Network Anomaly - Date Time (UTC) - Minute < 30 OR Network Anomaly - Date Time (UTC)
 - Minute > 35 )
```

Actions découlant d'une règle

Action	Description
ENREGISTRER	Les événements correspondants contribuent à la note d'anomalie de réseau et peuvent être trouvés à l'aide du tableau de bord de sécurité ou de la Onglet Network Anomalies (Anomalie de réseau)
ALERTE	Les événements correspondants s'affichent sur la page Alertes actuelles (Alertes) et dans les Choisir les serveurs de publication d'alertes (Serveurs de publication d'alertes) choisis.

La section suivante décrit plus en détail où trouver les événements d'anomalie de réseau détectés dans l'interface utilisateur.

Où voir les événements d'anomalies de réseau

Note Les événements d'anomalies de réseau ne sont actuellement *pas* affichés sur la page d'analyse criminalistique. Vous pouvez trouver les événements d'anomalies de réseau dans les pages suivantes.

- **Tableau de bord de sécurité :** les événements d'anomalies de réseau qui correspondent aux règles avec l'action **RECORD** (ENREGISTRER) se trouvent dans la section de la note d'anomalies de réseau dans le tableau de bord de la sécurité. S'il y a des charges de travail avec des notes différentes (inférieures à 100), en cliquant sur le nom de la charge de travail, vous pouvez afficher les séries chronologiques du PCR et les événements d'anomalies de réseau sur cette charge de travail. Sur le côté droit de chaque ligne du tableau des événements d'anomalie de réseau, vous pouvez voir des liens d'action qui peuvent vous aider à rechercher des flux et d'autres événements criminalistiques intervenus au moment de l'événement d'anomalie de réseau correspondant. Consultez la section Latence des anomalies de réseau pour connaître le retard connu du signalement dans la note d'anomalies de réseau.

Figure 357: Note d'anomalie de réseau dans le tableau de bord de la sécurité

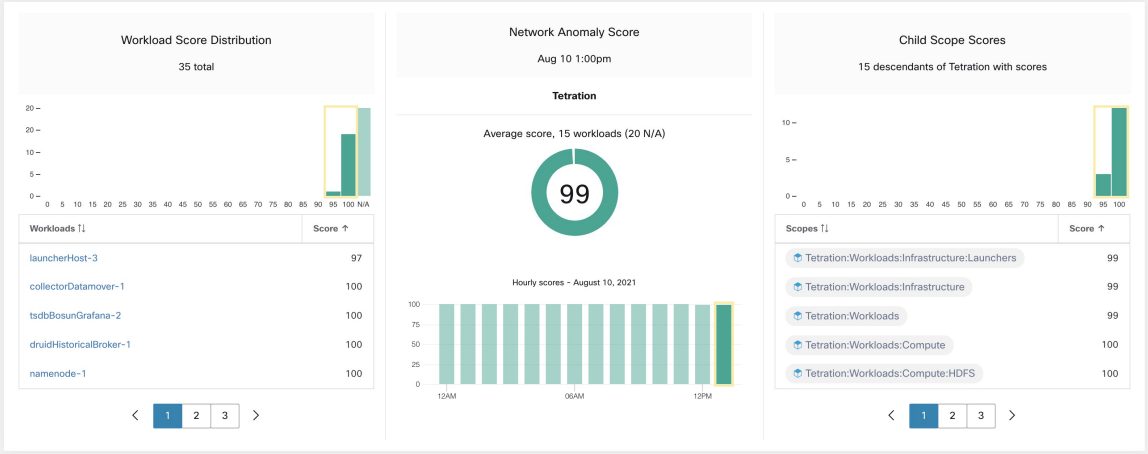
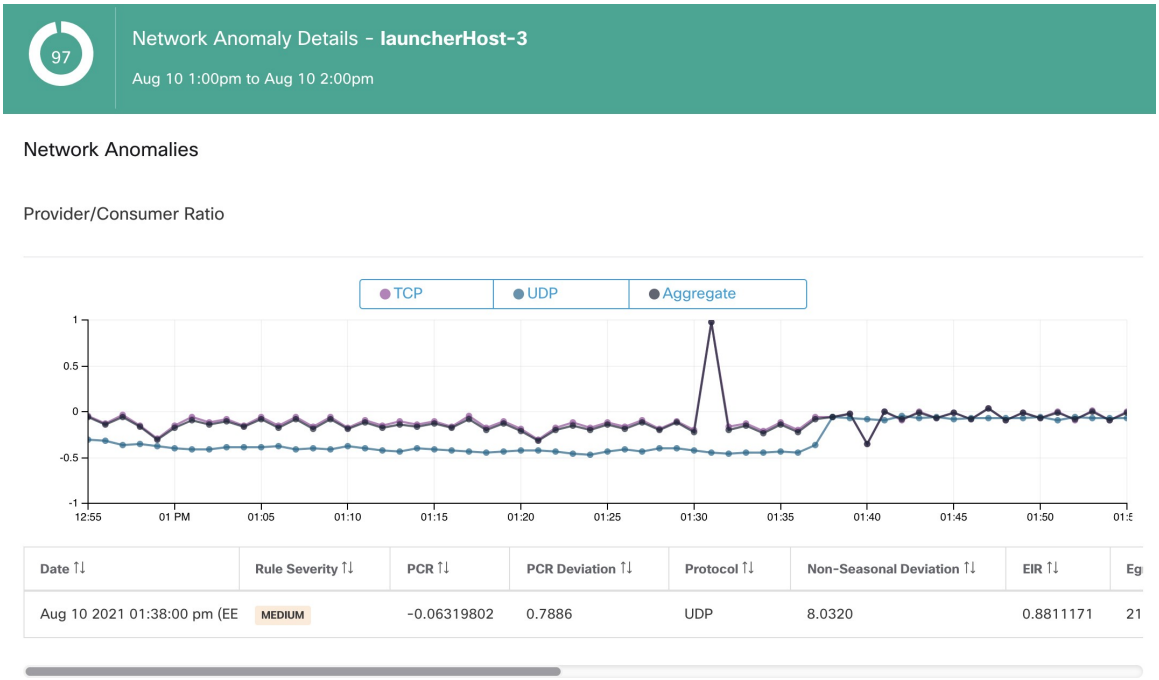
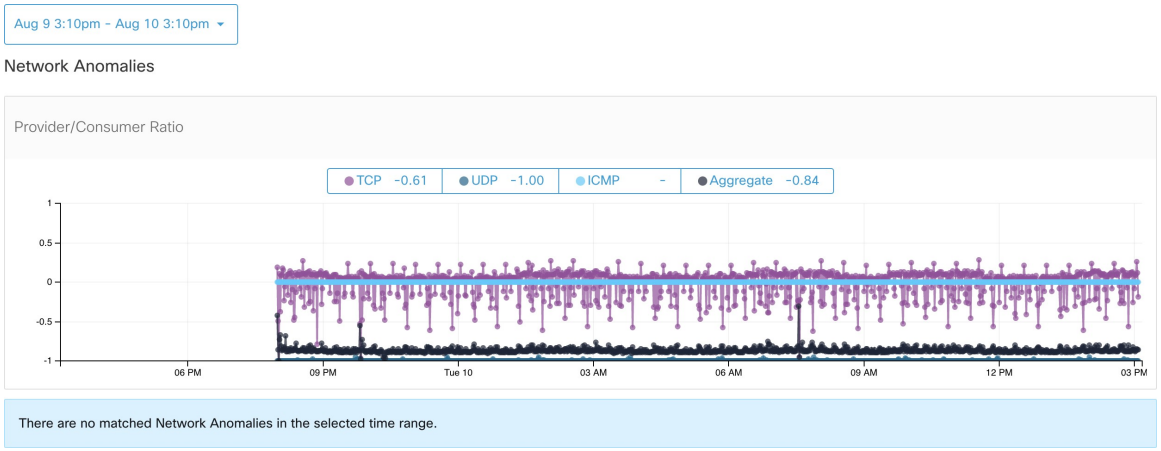


Figure 358: Note d'anomalie de réseau dans le tableau de bord de la sécurité, par charge de travail



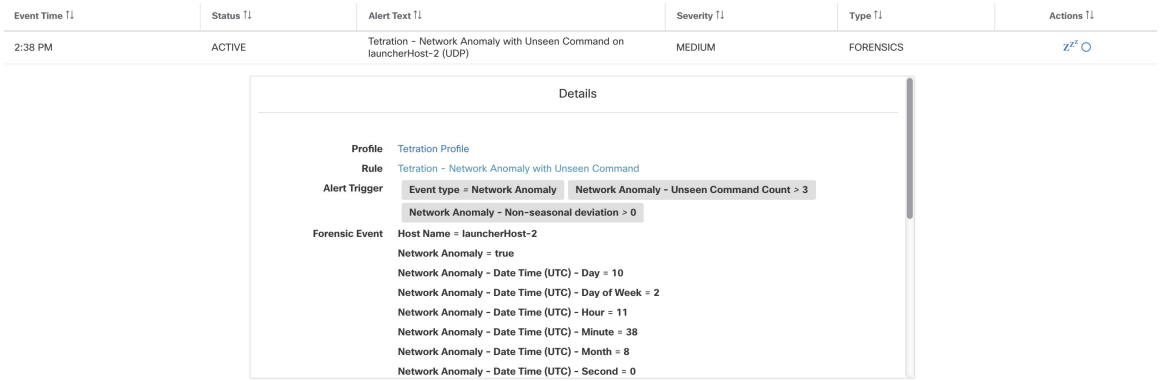
- Onglet Network Anomalies (Anomalie de réseau) **:** sur cette page, vous pouvez voir le graphique de la série chronologique PCR et les événements d'anomalie de réseau qui correspondent aux règles de l'action **RECORD** (ENREGISTRER). Ce que vous pouvez voir sur cette page est similaire à ce que vous trouvez en cliquant sur le nom de la charge de travail dans le tableau de bord de la sécurité.

Figure 359: Onglet Anomalie de réseau dans la page du Profil de charge de travail



- **Alertes :** Si la règle d'anomalie de réseau est configurée avec l'action **ALERT** ALERTE), les événements correspondants sont affichés dans la Alertes actuelles et sont également disponibles sur le serveur de publication d'alertes.

Figure 360: Alerte d'anomalie de réseau



Notes de gravité des règles et d'anomalies de réseau

Le calcul de la note d'anomalie de réseau est similaire à celui de la note criminalistique. Pour chaque charge de travail, nous calculons un niveau d'anomalie de réseau. Le score d'anomalie de réseau d'une charge de travail est dérivé des événements d'anomalie de réseau observés sur cette charge de travail en fonction des profils activés pour cette portée. Une note de 100 signifie qu'aucun événement d'anomalie de réseau n'a été observé par le biais des règles configurées dans les profils activés. Une note de 0 signifie qu'une anomalie de réseau a été détectée et nécessite une action immédiate.

- Un événement d'anomalie de réseau avec le niveau de gravité REQUIRES IMMEDIATE ACTION (NÉCESSITE UNE ACTION IMMÉDIATE) réduit la note pour l'ensemble de la portée à 0.
- Un événement d'anomalie de réseau avec le niveau de gravité CRITICAL (CRITIQUE) réduit la note de la charge de travail avec un impact de 10.
- Un événement d'anomalie de réseau avec un niveau de gravité HIGH (ÉLEVÉ) réduit la note de la charge de travail avec un impact de 5.

- Un événement d'anomalie de réseau avec le niveau de gravité MEDIUM (MOYEN) réduit la note de la charge de travail avec un impact de 3.
- Un événement d'anomalie de réseau avec la gravité LOW (FAIBLE) ne contribue pas à la note d'anomalie de réseau. Cela est recommandé pour les nouvelles règles lorsque la qualité du signal est toujours en cours d'optimisation et est susceptible d'être bruitée.

Pour chaque charge de travail, la note totale d'impact est agrégée toutes les 5 minutes pour calculer la note de cette charge de travail au cours de ces 5 minutes.

Pour les charges de travail sans types de capteurs activés pour les anomalies de réseau, les notes d'anomalie de réseau sont S.O.

Rétention des données PCR et des événements d'anomalies de réseau

Les données de PCR et les événements d'anomalie de réseau sont conservés pendant 7 jours.

Latence des anomalies de réseau

Les notes d'anomalie de réseau signalées dans le tableau de bord de sécurité ont des retards de 5 minutes. Par exemple, la note d'une charge de travail pour l'heure 10 h à 10 h 59 est basée sur les événements d'anomalie de réseau qui se produisent entre 9 h 55 et 10 h 54

Mises en garde

- Les anciens événements de fuite de données demeurent des événements de fuite de données au lieu d'événements d'anomalie de réseau.
- La détection des anomalies de réseau par protocole est une nouvelle fonctionnalité dans la version 3.3 et le protocole n'est pas défini dans les anciens événements de fuite de données.

Process hash anomaly detection

As the name suggested, this feature detects process hash anomaly by assessing the consistency of process binary hashes across the system. The motivation of this feature is as follows. Imagine that you have a farm of Apache web servers that are cloned from the same setup configuration (e.g., those servers are deployed from the same automation scripts). Then you would expect that the hashes of httpd binaries on all servers are the same. If there is a mismatch, it is an anomaly and might worth a further investigation.

Formally, we define *process group* as the set of processes across workloads in the same rootscope that have the same combination of executable binary path, OS version, and package info (if applicable)1.

Note Package info is included since 3.4 release; in the previous releases, the process group is defined based on the combination of executable binary path and OS version only.

In the example above, suppose that all Apache web servers are running httpd 2.4.43 on CentOS 7.7 and in the same rootscope, then the corresponding process group is the set of processes (across all servers) that have

the same combination: binary path of `/usr/sbin/ httpd` & OS version of `CentOS-7.7` & package version of `httpd-2.4.43`. It is expected that the hashes of all binaries in the same process group are the same, and an anomaly will appear if any mismatch is detected.

Besides detecting anomalous process hashes, this feature also detects process hashes that appear in a Flagged list Condensés de fichiers téléversés par l'utilisateur by user. The motivation is that you may have a list of known malware hashes, and would like to know if a process associated with any of those hashes is run.

To reduce false alarms, we use the National Software Reference Library's Reference Data Set (RDS) provided by NIST (we also call it NIST RDS dataset) as a Benign list; a benign hash is considered "safe" (see Analyse des rapports d'informations sur les menaces, on page 825 on how to enable NIST RDS dataset). You can also Condensés de fichiers téléversés par l'utilisateur your own hash Benign list.

In addition to the NIST RDS dataset, we also curate **Secure Workload Hash Verdict** service. When this service is enabled, if any known malware hash shows up, it will be detected as malicious hash. On the other hand, if the hash is known and legit, then it is also marked as benign in the anomaly analysis. Due to the extremely large dataset and fast updates that covers all known and legit process hashes that can be used to either approve or red flag processes running on a workload, Cisco Secure Workload Hash Verdict is only available via Cisco Secure Workload Cloud. Please refer to Mises à jour automatiques to ensure Cisco Secure Workload Hash Verdict service is accessible from your appliance.

Output of this feature is a security score called **process hash score**. This score is calculated and output hourly. Like all other security scores, a higher process hash score is better. In particular, for a process hash:

- Hash score of 0 means that the hash is flagged or malicious
- Hash score of 100 means that the hash is either benign, or consistent across workloads (no mismatch)
- Hash score from 1 to 99 means that the hash is considered anomalous (i.e., there is some mismatch)

The process hash score of an workload is the minimum process hash score of all hashes observed in that workload, with 0 meaning there is a flagged or malicious process hash in the system, and 100 meaning there is no hash anomaly observed in the system.

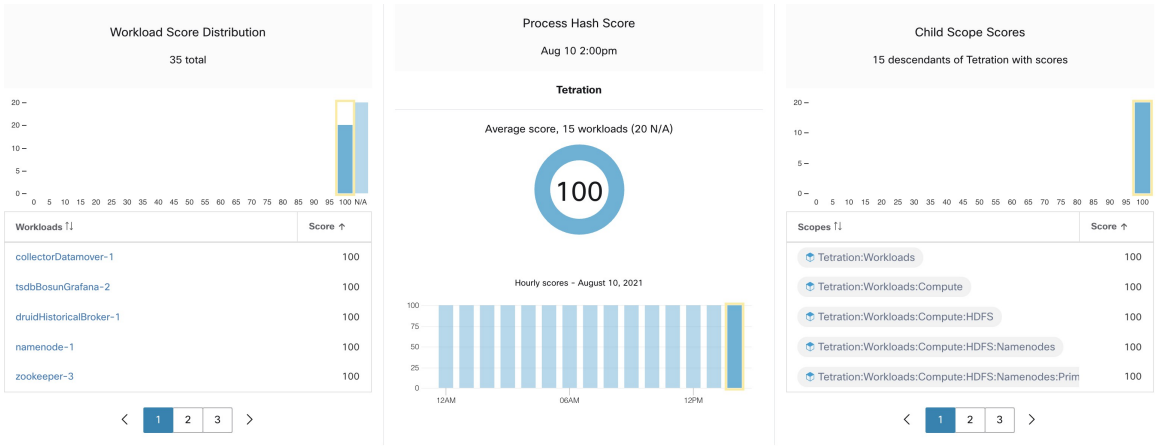
Comment activer la fonctionnalité de condensé de processus

La fonction de condensé de processus est activée par défaut sur les agents de visibilité approfondie et les agents d'application; aucune configuration criminalistique n'est nécessaire. Si de tels agents sont présents dans votre système, vous devriez commencer à voir les résultats dans les 2 heures suivant le démarrage du système.

Où voir la note de condensé de processus

- **Tableau de bord de sécurité**

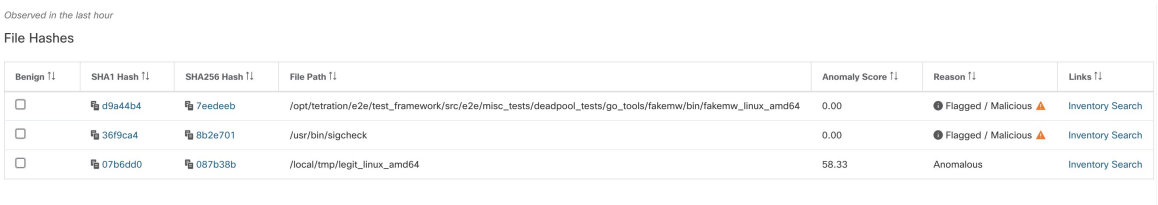
Figure 361: Traiter la section de la note de condensé dans le Tableau de bord de sécurité



Traiter la section de la note de condensé dans le Afficher le Tableau de bord de sécurité

- **Page du profil de la charge de travail** / Onglet Condensés de fichiers :

Figure 362: Onglet Condensé du fichier dans la page de Profil de charge de travail



Onglet Condensé du fichier dans la Profil de la charge de travail

Comment la note de condensé de processus est calculée

Pour chaque condensé de processus, nous calculons une note comme suit :

1. Si le condensé est signalé ou malveillant, `note = 0`
2. Sinon, si le condensé est inoffensif, `note = 100`
3. Sinon, si le condensé est en anomalie, la `note` est comprise dans la plage `[1, 99]`, plus elle est élevée, mieux c'est.
4. Sinon, `note = 100`

La logique de calcul de la note dans (3) est la suivante : nous calculons d'abord la note minimale du condensé (qui est égale à un moins le ratio de population de ce condensé dans la population de charge de travail sous la même portée), puis nous l'inscrivons dans l'intervalle `[0,0, 1,0]` à l'aide d'une fonction d'information `-log2(x)`. Si la note minimale du condensé est supérieure à 0,5, nous inscrivons à nouveau la note dans l'intervalle `[1,0, 99,0]`. Prenons l'exemple de la batterie de serveurs Web Apache ci-dessus et considérons le condensé de `httpd`. Voici quelques scénarios :

- Supposons que `httpd` ait deux valeurs de condensé (`h1` et `h2`) sur 1 000 serveurs de la batterie : `h1` sur 1, `h2` sur les 999 autres serveurs. Dans ce cas :

- `population_ratio(h1) = 0,001, population_ratio(h2) = 0,999`. Ensuite :
- `minority_score(h1) = 0,999,minority_score (h2) = 0,001`. Ensuite :
- `note (h1) = -log2 (0,999) * 98 +1 = 1,14;`
- Puisque `minority_score(h2) < 0,5, h2` n'est pas considéré comme une anomalie, alors `score(h2) = 100`.

- Supposons que `httpd` ait deux valeurs de condensé (`h1` et `h2`) sur 10 serveurs de la batterie : `h1` sur 1 serveur, `h2` sur les 9 autres serveurs. Dans ce cas :
  - `population_ratio(h1) = 0,1 = population_ratio(h2) = 0,9`. Ensuite :
  - `minority_score(h1) = 0,9, minority_score(h2)= 0,1`. Ensuite :
  - `note(h1) = -log2 (0,9) * 98 +1 = 15,90;`
  - Puisque `minority_score(h2) < 0,5, h2` n'est pas considéré comme une anomalie, alors `score(h2) = 100`.

- Supposons que `httpd` comporte deux valeurs de condensé (`h1` et `h2`) sur deux serveurs de la batterie : `h1` sur un serveur, `h2` sur l'autre. Dans ce cas :
  - `population_ratio(h1) = population_ratio(h2) = 0,5`. Ensuite :
  - `minority_score(h1) = minority_score(h2) = 0,5`. Ensuite :
  - `score(h1) = score(h2) = -log2(0,5) * 98 + 1 = 99,0`. Il s'agit du score le plus élevé pour un condensé qui est considéré comme une anomalie.

- Supposons que `httpd` n'ait qu'une seule valeur de condensé (`h1`) sur tous les serveurs. Dans ce cas, `minority_score(h1) = 0,0 < 0,5;` par conséquent, il n'est pas considéré comme une anomalie et son `score(h1) = 100`.

Enfin, la note de condensé de processus d'une charge de travail est la note de condensé de processus minimale de tous les condensés observés dans cette charge de travail.

Vous pouvez trouver ici des renseignements supplémentaires sur la fonction d'information `-log2(x)`.

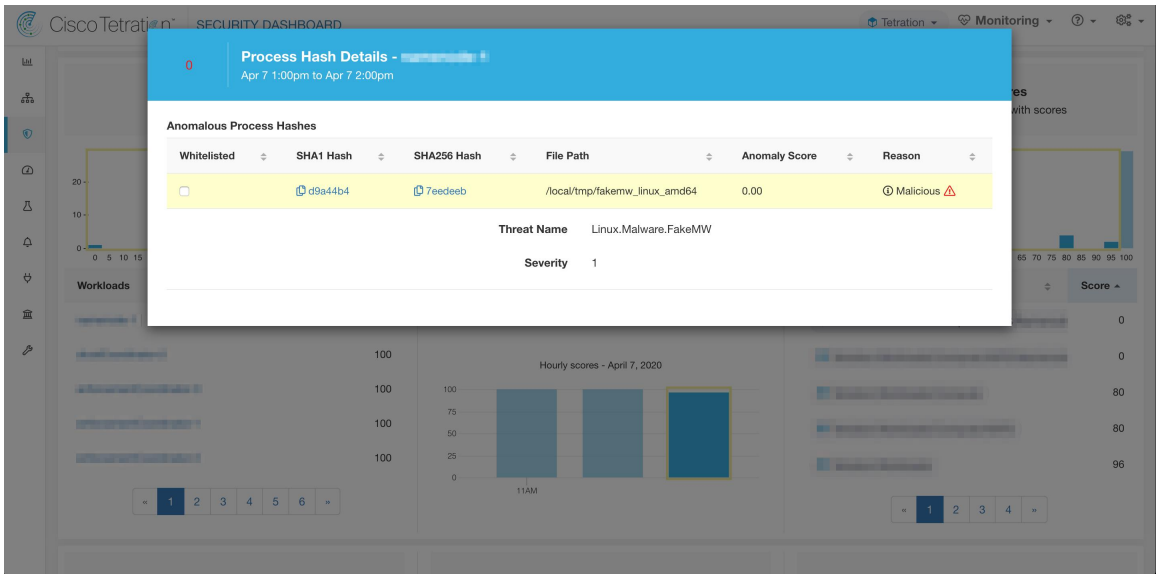
Comment améliorer la note de condensé de processus

Une note de condensé de processus de 0 pour une charge de travail signifie qu'un condensé de processus signalé ou malveillant est apparu dans cette charge de travail; le fait d'empêcher ce processus de s'exécuter à nouveau améliore le résultat. Une note de condensé de processus positive inférieure à 100 signifie qu'il y a une anomalie de condensé de processus dans votre système; ce n'est pas malveillant mais mérite une enquête plus approfondie. Après une enquête approfondie, s'il est conclu que le condensé est sûr, l'ajouter à votre liste « Bénigne » améliorera également le résultat. L'utilisateur peut marquer les condensés anormaux comme « bénins » en cochant la case « Bénin » dans la page File Hashs/Process Hash Details (Détails des condensés de fichiers/processus) ou en Condensés de fichiers téléversés par l'utilisateur.

Détails sur la menace

Comme mentionné précédemment, si Cisco Secure Workload, le service Hash Verdict (Verdict de condensé) est activé, tout condensé de logiciel malveillant connu, lorsqu'il apparaît, est signalé comme malveillant. Dans ce cas, des informations supplémentaires sur les menaces du condensé malveillant (recueillies sur notre plateforme de renseignements sur les menaces) sont fournies. Actuellement, les données supplémentaires sur les menaces comprennent le *nom* et *la gravité* de la menace. Le nom est le nom de la menace, tandis que la gravité est une valeur comprise entre 1 et 5 pour indiquer sa gravité, où 1 signifie la menace la moins grave et 5 la plus grave.

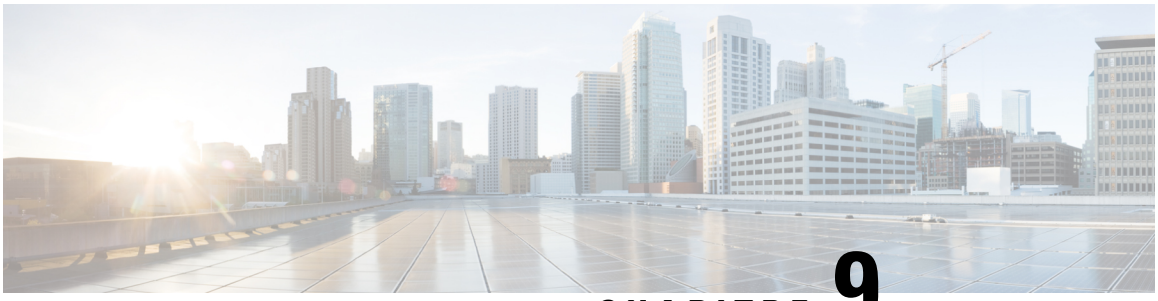
Figure 363: L'utilisateur peut cliquer sur la ligne contenant le code de condensé malveillant pour afficher les détails des renseignements sur les menaces



Mises en garde

- La tâche d'analyse du condensé des processus est exécutée une fois par heure, mais il peut s'écouler jusqu'à deux heures avant que les notes/résultats attendus ne s'affichent dans le tableau de bord de la sécurité, en fonction de l'action. Voici des exemples :
  - Si vous chargez votre liste de condensés marqués et qu'un condensé de processus figurant dans cette liste apparaît, il peut s'écouler jusqu'à une heure avant que la note ne soit reflétée dans le tableau de bord de la sécurité.
  - Si vous supprimez un condensé de votre liste marquée, il peut s'écouler jusqu'à deux heures avant qu'il soit effacé et que le résultat soit reflété dans le tableau de bord de sécurité.
- Conservation :
  - Les résultats détaillés de l'analyse de condensé de processus sont conservés pendant au moins 7 jours.
- L'onglet File Hashs (Condensés de fichiers) dans la page Workload Profile (Profil de charge de travail) affiche uniquement les détails du condensé de processus analysés au cours de la dernière heure.

- Les versions précédentes des agents de visibilité approfondie et d'application, et les points d'accès AnyConnect signalaient uniquement les valeurs de condensé SHA256. Par conséquent, la correspondance avec la liste marquée/bénigne du condensé SHA1 n'est pas prise en charge pour ces agents.
- La note de condensé de processus est calculée en fonction d'une portée racine particulière. Si une charge de travail appartient à plusieurs portées racine, la note de condensé de processus de cette charge de travail est la note minimale de toutes les portées racine auxquelles elle appartient.
- Pour réduire davantage les fausses alertes lors de l'analyse des anomalies de condensé de processus, nous marquons également tous les fichiers binaires Cisco Secure Workloadcomme bénins en fonction de leurs chemins d'accès à leurs fichiers. Ce mécanisme se produit uniquement lorsque ces condensés n'apparaissent dans aucune liste de condensé définie par l'utilisateur ou ne sont pas signalés par le service Hash Verdict Cisco Secure Workload.



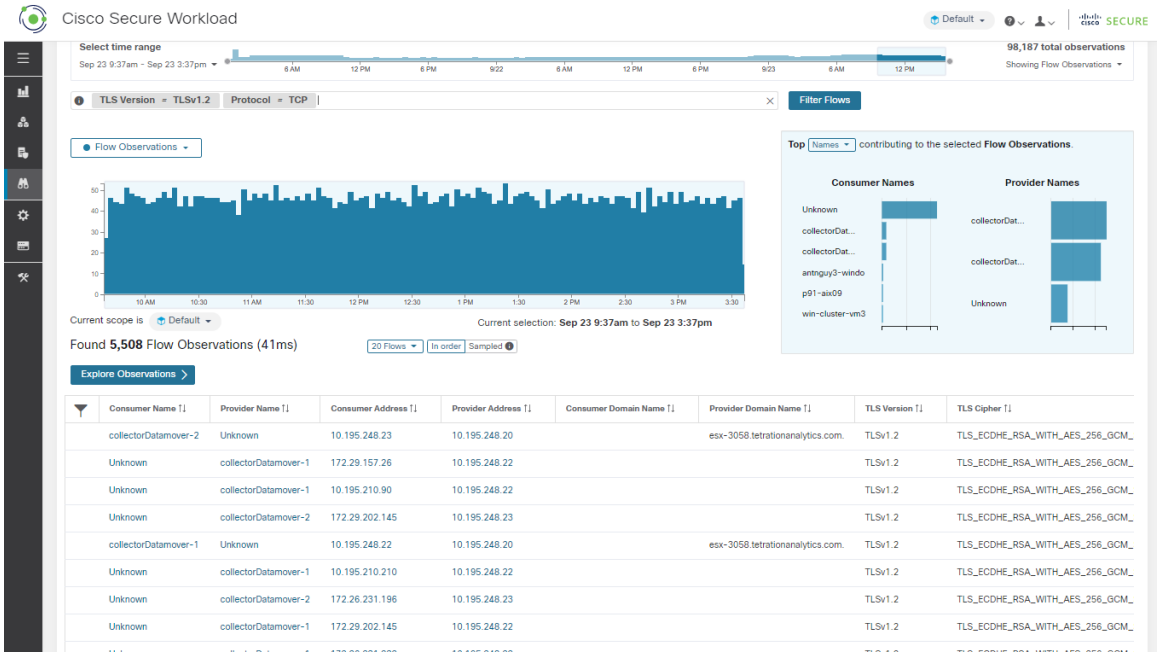
CHAPITRE 9

Flux de réseau – Visibilité du trafic

Sur l'interface utilisateur de Cisco Secure Workload, dans le volet de navigation, choisissez **Investigate (Enquêter)** > **Traffic (Trafic)** qui permet d'accéder à la page de recherche de flux. Cette page fournit les moyens de filtrer et d'explorer rapidement le contenu des flux. L'unité de base est **Flow Observation** (l'observation de flux), qui est une agrégation par minute de chaque flux unique. Les deux côtés du flux sont appelés **Consumer** (consommateur) et **Provider** (fournisseur), le consommateur lance le flux et le fournisseur répond au consommateur (par exemple, **client** et **serveur** respectivement). Chaque observation suit le nombre de paquets, d'octets et autres mesures dans chaque direction pour ce flux et pendant cet intervalle d'une minute. En plus de permettre un filtrage rapide, les flux peuvent être explorés visuellement à l'aide des **Explore Observations** (observations Explore). Vous pouvez cliquer sur la liste d'observations de flux qui en résulte pour afficher les détails de ce flux, y compris la latence, les paquets et les octets sur la durée de vie de ce flux.

Avertissement Pour les hôtes dotés d'agents de visibilité approfondie oud'application, Cisco Secure Workload est en mesure de corréler les données de flux avec le processus qui fournit ou consomme le flux. Par conséquent, les arguments de ligne de commande complets, qui peuvent inclure **des informations sensibles telles que les informations d'authentification de la base de données ou de l'API**, utilisés pour lancer le processus sont disponibles pour l'analyse et l'affichage.

Illustration 364 : Présentation des flux



Sélecteur de corpus

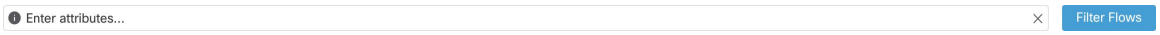
Figure 365: Sélecteur de corpus

Il s'agit des données chronologiques sommaires non filtrées pour la **portée** actuelle pour l'ensemble du corpus. Le but de ce composant est de vous permettre de savoir quelle plage de dates est affichée et de modifier facilement cette plage de dates en la faisant glisser dans le composant. Les données du tableau sont présentes pour le cas où elles seraient utiles pour décider quelle plage temporelle sélectionner. Vous pouvez sélectionner différentes mesures à afficher (par défaut, le nombre d' **observations de flux** est affiché).

Le sélecteur de corpus peut actuellement prendre en charge la sélection d'*environ* **2 milliards d'observations de flux**.

Colonnes et filtres

Figure 366: Filtrer l'entrée



C'est ici que vous définissez les filtres pour affiner les résultats de la recherche. Cliquez sur l'icône **(?)** à côté du mot **Filters** (filtres) pour afficher toutes les dimensions possibles. Pour toutes les données d'étiquettes d'utilisateur, ces colonnes sont également disponibles pour les intervalles appropriés. Cette entrée prend également en charge les mots-clés **and**, **or**, **not** et **parenthesis**, utilisez-les pour concevoir des filtres plus complexes. Par exemple, un filtre indépendant de la direction entre IP *1.1.1.1* et *2.2.2.2* peut s'écrire :

Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1

Et pour filtrer également sur Protocol = TCP :

(Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1) and Protocol = TCP

L'entrée du filtre prend également en charge les « , » et « - » pour le port, l'adresse du client et l'adresse du fournisseur, en transformant « - » en requêtes de plages. Voici des exemples de filtres valables :

Figure 367: Prise en charge de l'entrée du filtre pour l'adresse du consommateur

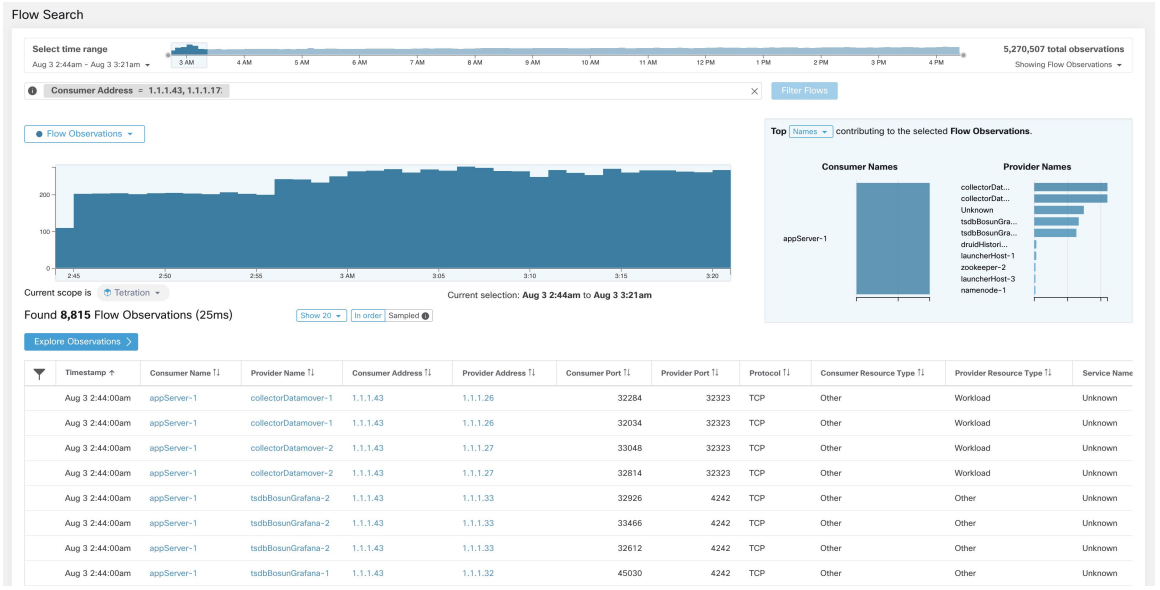


Figure 368: L'entrée du filtre prend en charge la requête de plage pour l'adresse du consommateur

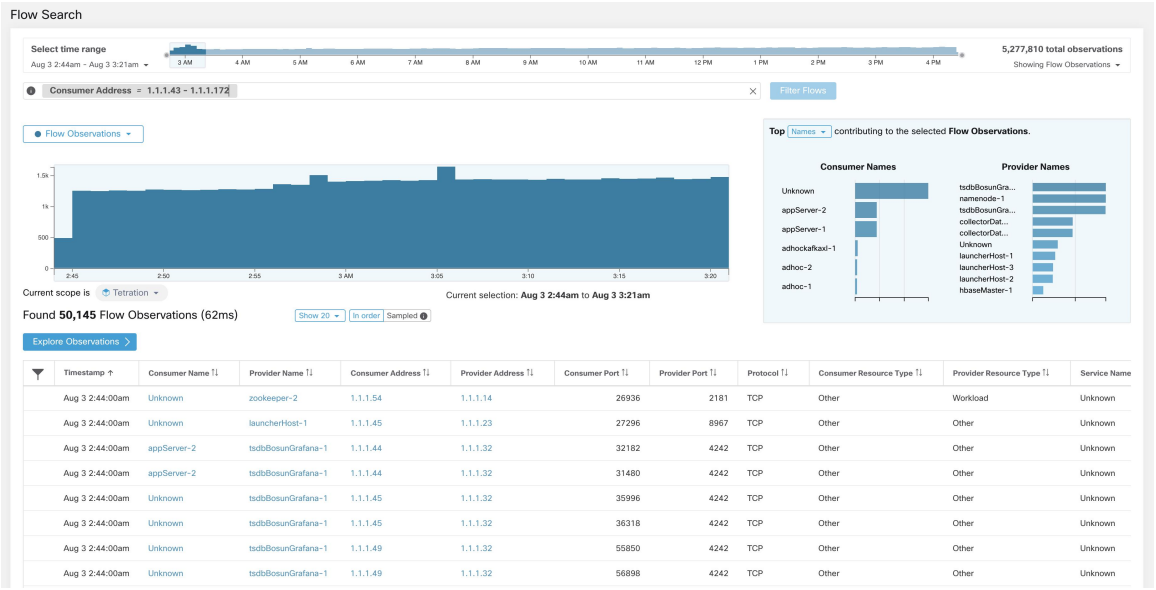


Table 33: Colonnes et filtres disponibles

Colonnes (noms affichés dans l'API)	Description	Source
Adresse du consommateur (*src_address*)	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24). Correspond aux observations de flux dont l'adresse du consommateur recouvre l'adresse IP ou le sous-réseau fourni.	Agents logiciels et dispositifs d'acquisition
Adresse du fournisseur (*dst_address*)	Saisissez un sous-réseau ou une adresse IP au moyen de la notation CIDR (par exemple, 10.11.12.0/24) Correspond aux observations de flux dont l'adresse du fournisseur recouvre l'adresse IP ou le sous-réseau fourni.	Agents logiciels et dispositifs d'acquisition
Consumer Name	Recherche les observations de flux dont le nom de la charge de travail du consommateur recouvre le nom de la charge de travail du consommateur saisi.	Agents logiciels et connecteur AnyConnect
Provider Name	Recherche les observations de flux dont le nom de la charge de travail du fournisseur recouvre le nom de la charge de travail du fournisseur saisi.	Agents logiciels et connecteur AnyConnect
Utilisateur consommateur	Recherche les observations de flux dont le nom du consommateur recouvre le nom du consommateur qui a généré le flux.	Agents logiciels et connecteur AnyConnect
Utilisateur fournisseur	Recherche les observations de flux dont le nom du fournisseur recouvre le nom du fournisseur saisi qui a géré le flux.	Agents logiciels et connecteur AnyConnect

Colonnes (noms affichés dans l'API)	Description	Source
Nom de domaine du consommateur	Recherche les observations de flux dont le nom de domaine client (associé à l'adresse IP du client ou au sous-réseau) recouvre le nom de domaine client saisi.	Agents logiciels et connecteur AnyConnect
Nom de domaine du fournisseur	Recherche les observations de flux dont le nom de domaine du fournisseur (associé à l'adresse IP ou au sous-réseau du fournisseur) recouvre le nom de domaine du fournisseur saisi.	Agents logiciels et connecteur AnyConnect
Nom d'hôte du consommateur (*src_hostname*)	Correspond aux flux dont le nom d'hôte du consommateur recouvre le nom d'hôte fourni.	Agents logiciels et connecteur AnyConnect
Nom d'hôte du fournisseur (*dst_hostname*)	Recherche les flux dont le nom d'hôte du fournisseur recouvre le nom d'hôte fourni.	Agents logiciels et connecteur AnyConnect
Groupe d'application du consommateur (*src_enforcement_epg_name*)	Le groupe d'application du consommateur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques appliquées qui correspond au consommateur.	Interne
Groupe d'application du fournisseur (*dst_enforcement_epg_name*)	Le groupe d'application du fournisseur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques appliquées qui correspond au fournisseur.	Interne
Groupe d'analyse du consommateur	Le groupe d'analyse du consommateur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques analysées qui correspond au consommateur.	Interne
Groupe d'analyse des fournisseurs	Le groupe d'analyse du fournisseur est le nom du filtre (portée, filtre d'inventaire ou grappe) dans les politiques analysées qui correspond au fournisseur.	Interne
Portée du consommateur (*src_scope_name*)	Correspond aux flux dont le consommateur appartient à la portée spécifiée.	Interne
Portée du fournisseur (*dst_scope_name*)	Correspond aux flux dont le fournisseur appartient à la portée spécifiée.	Interne
Port du consommateur (*src_port*)	Correspond aux flux dont le port de consommateur recouvre le port fourni.	Agents logiciels, ERSPAN et NetFlow
Port du fournisseur (*port_dst*)	Correspond aux flux dont le port du fournisseur recouvre le port fourni.	Agents logiciels, ERSPAN et NetFlow

Colonnes (noms affichés dans l'API)	Description	Source
Pays du consommateur (*src_country*)	Correspond aux flux dont le pays du consommateur recouvre le pays fourni.	Interne
Pays du fournisseur (*dst_country*)	Correspond aux flux dont le pays du fournisseur recouvre le pays fourni.	Interne
Subdivision du consommateur (*src_subdivision*)	Correspond aux flux dont la sous-division du consommateur recouvre la sous-division fournie ((État).	Interne
Subdivision du fournisseur (*dst_Subdivision*)	Correspond aux flux dont la sous-division du fournisseur recouvre la sous-division fournie (État).	Interne
Organisation du système autonome du consommateur (*src_ autonomous_system_organization*)	Correspond aux flux dont l'organisation du système autonome du consommateur recouvre l'organisation du système autonome (ASO) fourni.	Interne
Organisation du système autonome du fournisseur (*dst_autonomous_system_organisation*)	Correspond aux flux dont l'organisation du système autonome du fournisseur recouvre l'organisation du système autonome (ASO) fourni.	Interne
Protocole (*proto*)	Filtrez les observations de flux par type de protocole (TCP, UDP, ICMP).	Agents logiciels et dispositifs d'acquisition
Type d'adresse (*key_type*)	Filtrez les observations de flux par type d'adresse (IPv4, IPv6, DHCPv4).	Agents logiciels et dispositifs d'acquisition
Indicateurs TCP Avant	Filtrez les observations de flux par indicateurs (SYN, ACK, ECHO).	Agents logiciels, ERSPAN et NetFlow
Indicateurs TCP Retour	Filtrez les observations de flux par indicateurs (SYN, ACK, ECHO).	Agents logiciels, ERSPAN et NetFlow
UID de processus Avant (*fwd_process_owner*)	Filtrez les observations de flux par UID de propriétaire de processus (root, admin, yarn, mapred).	Agents logiciels
UID du processus Rev. (*rev_process_owner*)	Filtrez les observations de flux par UID de propriétaire de processus (root, admin, yarn, mapred).	Agents logiciels
Processus Avant (*fwd_process_string*)	Filtrez les observations de flux par processus (java, Hadoop, nginx). Voir l'avertissement relatif à la visibilité de la chaîne de processus	Agents logiciels

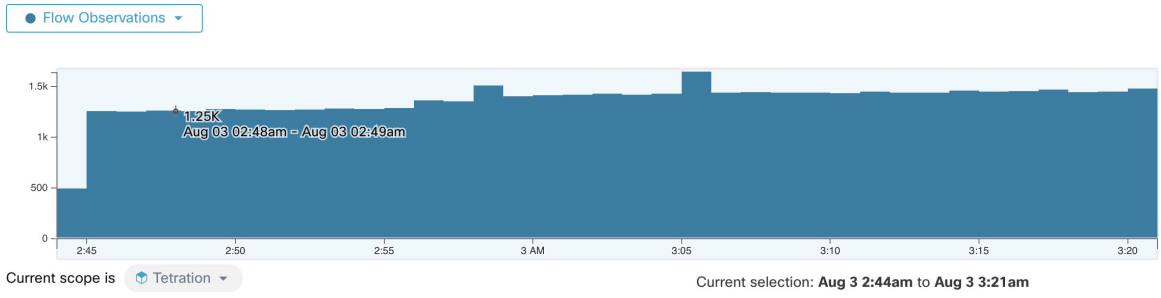
Colonnes (noms affichés dans l'API)	Description	Source
Processus Retour (*rev_process_string*)	Filtrez les observations de flux par processus (java, Hadoop, nginx). Voir l'avertissement relatif à la visibilité de la chaîne de processus	Agents logiciels
Consumer In Collection Rules?	Mettre en correspondance uniquement les consommateurs internes.	Interne
Provider In Collection Rules?	Mettre en correspondance uniquement les fournisseurs internes.	Interne
SRTT disponible	Met en correspondance les flux pour lesquels des mesures SRTT sont disponibles en utilisant les valeurs « vrai » ou « faux ». (Ceci équivaut à un SRTT > 0).	Interne
Octets	Filtrez les observations de flux par tranche de trafic d'octets. Correspond aux flux dont les valeurs de tranche de trafic d'octets sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Agent logiciel et appareils d'acquisition
Paquets	Filtrez les observations de flux par tranche de trafic de paquets. Correspond aux flux dont les valeurs de tranches de trafic de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel et appareils d'acquisition
Durée du flux (µs)	Filtrez les observations de flux par tranche de durée de flux. Correspond aux flux dont les valeurs de tranche de durée de flux sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Interne
Durée des données (µs)	Filtrez les observations de flux par tranche de durée des données. Correspond aux flux dont les valeurs de tranche de durée de données sont =, <, > (regroupées par puissances de 2 (0, 2, 64, 1024)).	Interne
SRTT (µs) (*srtt_dim_usec*)	Filtrez les observations de flux par tranche SRTT. Correspond aux flux dont les valeurs de tranches SRTT sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel
Retransmissions de paquets Avant (*fwd_tcp_pkts_retransmitted*)	Filtrez les observations de flux par tranches de retransmissions de paquets. Correspond aux flux dont les valeurs de tranches de retransmissions de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel
Retransmissions de paquets Retour (*rev_tcp_pkts_retransmitted*)	Filtrez les observations de flux par tranches de retransmissions de paquets. Correspond aux flux dont les valeurs de tranches de retransmissions de paquets sont =, <, > regroupées par puissance de 2 (0, 2, 64, 1024)).	Agent logiciel

Colonnes (noms affichés dans l'API)	Description	Source
Étiquettes d'utilisateur (* ou préfixe *user_*)	Données définies par l'utilisateur qui sont associées aux étiquettes personnalisées chargées manuellement qui commencent par * dans l'interface utilisateur et *user_* dans OpenAPI.	CMDB
TLS Version (Version TLS)	Version du protocole SSL utilisée dans le flux.	Agent logiciel
Chiffrement TLS	Type d'algorithme utilisé par le protocole SSL dans le flux.	Agent logiciel
Type d'agent du consommateur	Préciser le type d'agent de consommateur.	Interne
Type d'agent du fournisseur	Précisez le type d'agent du fournisseur.	Interne
Type de ressource consommateur	Représente le flux de ressources d'une source à un consommateur. Il peut s'agir d'une charge de travail, de pods, de services ou autres	Interne
Type de ressource de fournisseur	Représente le flux de ressources d'un fournisseur à un consommateur. . Il peut s'agir d'une charge de travail, de pods, de services ou autres.	Interne

Note Comme les données de flux sont marquées avec des étiquettes d'utilisateur uniquement au moment de l'acquisition, les étiquettes d'utilisateur ne s'affichent pas immédiatement après leur activation. Quelques minutes peuvent s'écouler avant que les étiquettes ne commencent à apparaître dans la recherche de flux. En outre, les étiquettes d'utilisateur disponibles varient en fonction de la partie du **sélecteur de corps** que vous avez sélectionnée, car les étiquettes activées peuvent avoir été modifiées à divers moments.

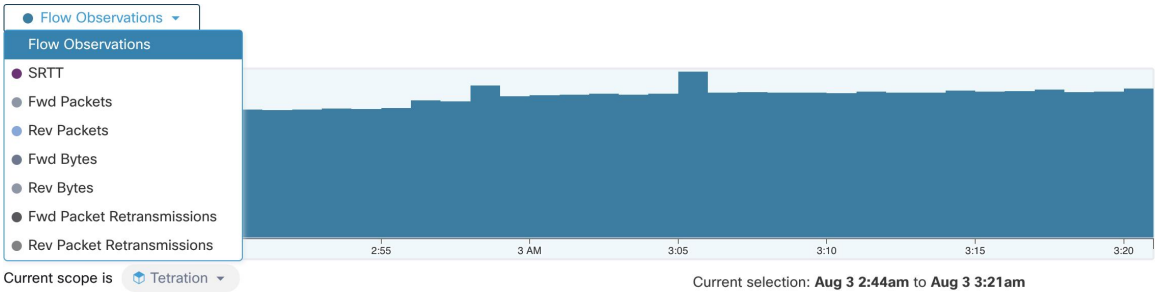
Séries temporelles filtrées

Figure 369: Séries temporelles filtrées



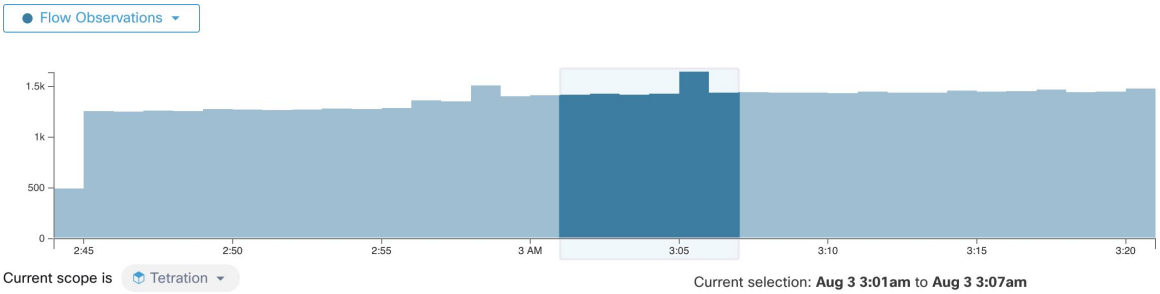
Ce composant affiche les totaux agrégés de diverses mesures pour l'intervalle sélectionné (sélection effectuée dans Sélecteur de corpus, on page 652). Utilisez la liste déroulante pour modifier la mesure à afficher.

Figure 370: Liste déroulante des séries chronologiques



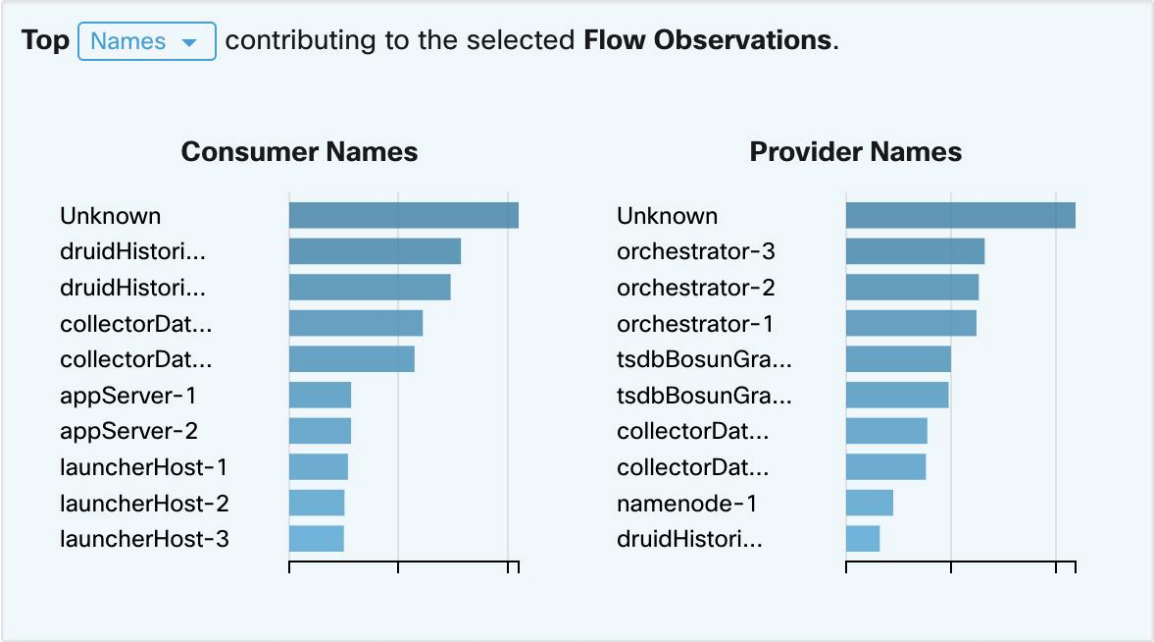
Il est également possible de réduire davantage l'intervalle sélectionné dans ce composant. Cliquez sur la zone du graphique sur laquelle vous souhaitez vous concentrer. Les N principaux graphiques et les données ci-dessous seront tous mis à jour pour inclure uniquement les données de l'intervalle sélectionné.

Figure 371: Séries chronologiques avec sélection



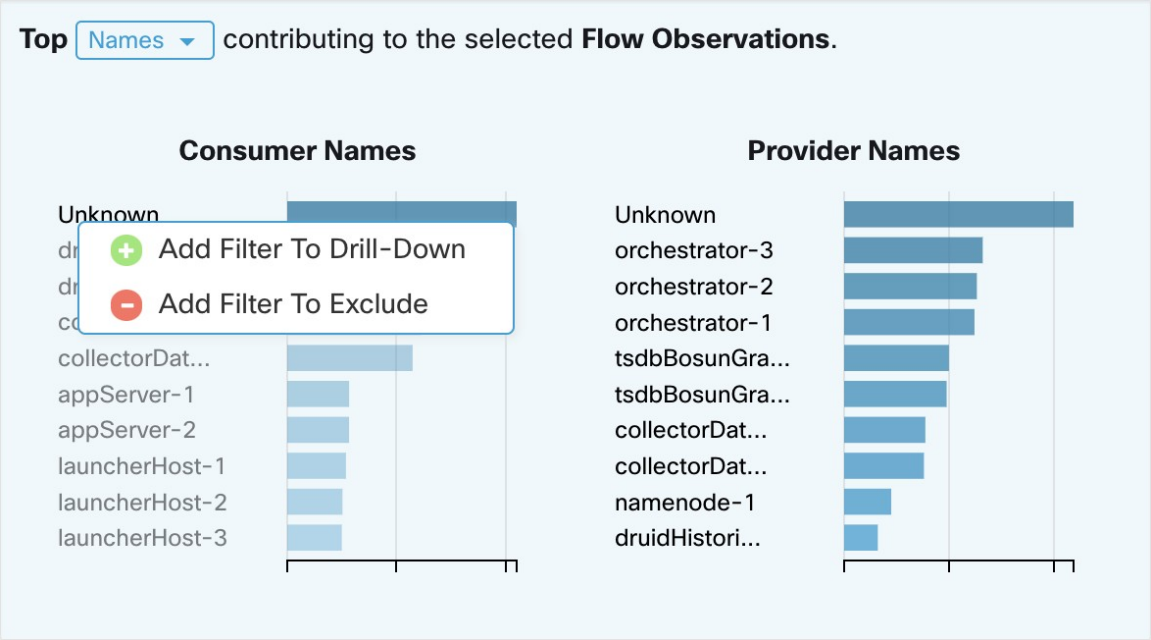
N principales valeurs

Figure 372: N principales valeurs



Les tableaux affichent les N valeurs les plus élevées qui contribuent à la sélection dans le graphique des séries chronologiques filtrées situé à gauche. La sélection d'un pic dans les observations de flux dans le tableau de séries chronologiques et de noms d'hôtes dans les tableaux des N principales valeurs, permet d'afficher la liste des noms d'hôte (consommateur et fournisseur) qui contribuent le plus à ces observations de flux. De plus, si le tableau de série chronologique est configuré pour afficher un SRTT, les principaux noms d'hôte affichent ceux qui contribuent le plus au SRTT sélectionné.

Figure 373: Approfondir/Exclure

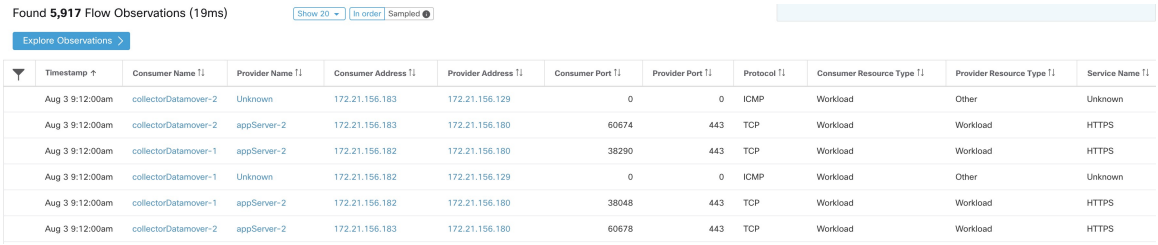


Cliquez sur l'un des éléments des tableaux des N principales valeurs pour afficher un menu qui vous permet d'**approfondir** ou d'**exclure** cette valeur.

- Cliquez sur **Drill-Down** (Approfondir) pour ajouter un filtre qui limite les résultats à cette valeur.
- Cliquez sur **Exclude** (Exclure) pour ajouter un filtre qui exclut cette valeur des résultats.

Note Après avoir cliqué sur **Approfondir** ou **Exclure**, vous devez appuyer sur l'icône **Filtrer** pour que le filtre prenne effet. Cela afin que plusieurs actions d **exclusion** puissent être effectuées rapidement sans que la page soit mise à jour à plusieurs reprises en même temps.

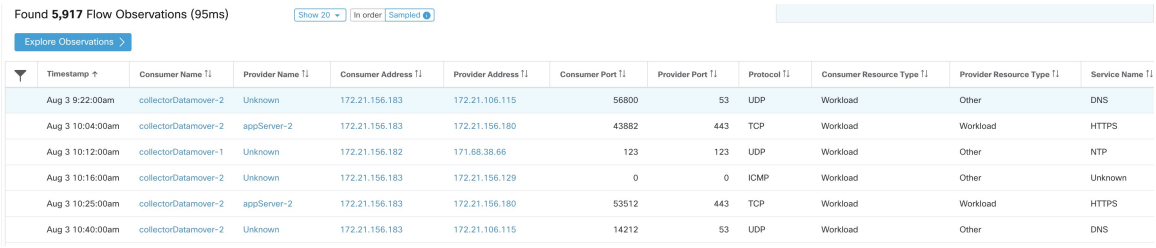
Liste d'observations



Ceci est la liste des **observations de flux** réelles qui correspondent aux filtres et aux sélections de la page ci-dessus. Par défaut, 20 fichiers seront chargés en commençant par le début de l'intervalle. Il est possible d'augmenter le nombre de fichiers chargés en utilisant la liste déroulante. Il est également possible de charger un ensemble aléatoire d'observations de flux à partir de l'intervalle sélectionné en utilisant la commande

Sampled (Échantillonné) plutôt que **In order** (Dans l'ordre). Le paramètre **Échantillonné** est utile pour obtenir un ensemble plus représentant d'observations de débit à partir de l'intervalle sélectionné plutôt que de les charger successivement à partir du début de l'intervalle.

Figure 374: Échantillonné



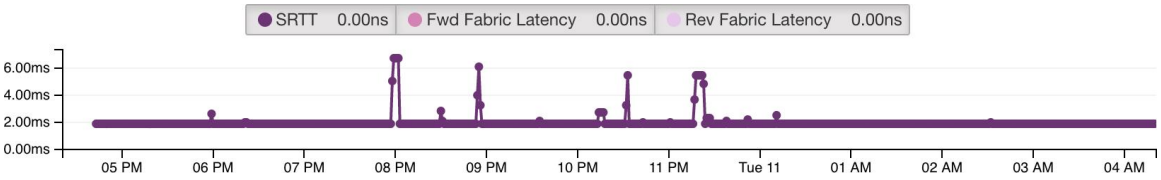
Détails des flux

Cliquez sur l'une des lignes pour développer la section **Flow Details** (détails d flux).es Cette fonction permet d'afficher un résumé du flux et des tableaux de diverses mesures pour la durée de vie de ce flux. Pour les flux de longue durée, un tableau récapitulatif s'affiche au bas de la page. Il vous permet de choisir différents intervalles pour lesquels afficher les données de séries chronologiques.

Figure 375: Détails des flux

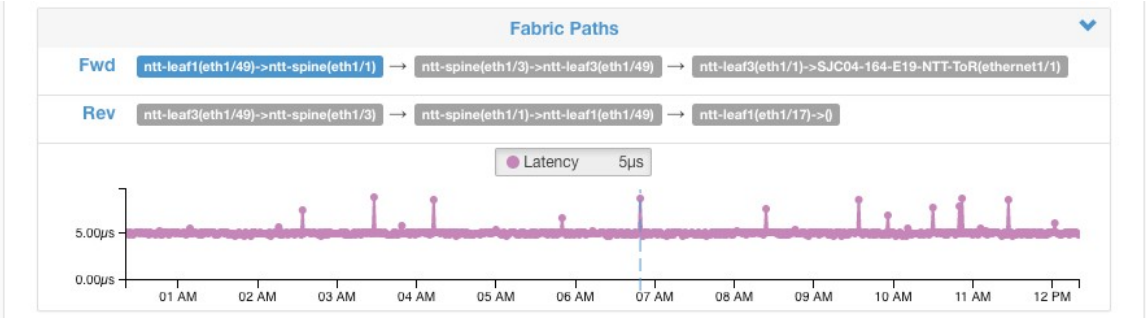
Pour les flux étiquetés avec des informations sur le chemin de la structure, **la latence de trame avant/retour** et **SRTT** sont disponibles. Les tableaux de séries chronologiques pour d'autres mesures, comme les **indicateurs de rafale avant/retour et les indicateurs de rafale avant/retour + Abandon,** peuvent être affichés s'ils sont disponibles. Reportez-vous à Compatibilité.

Figure 376: Latence



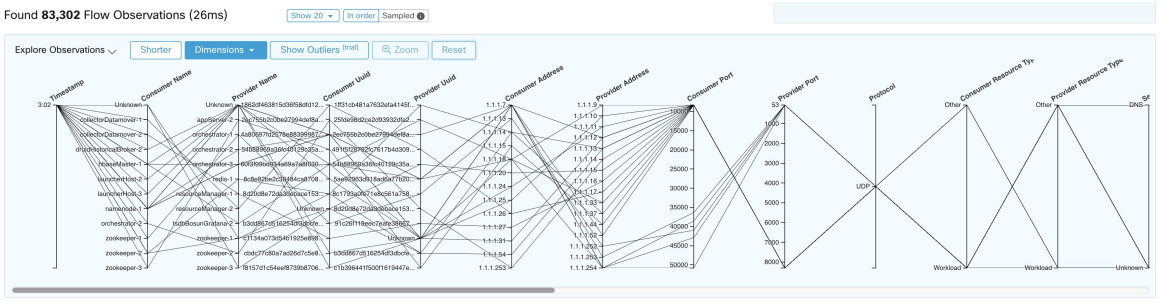
Des détails sur le **chemin de structure Avant/Retour** sont également disponibles. Chaque lien est cliquable, ce qui active les tableaux de série chronologique de **latence** et d'**abandon** (lorsqu'ils sont non nuls). Cliquez sur **Fwd** (Avant) ou **Rev** (Retour) pour accéder au détail de la page Fabric Path Overlay (Superposition de chemins de la structure) pour le flux.

Figure 377: Chemins de la structure



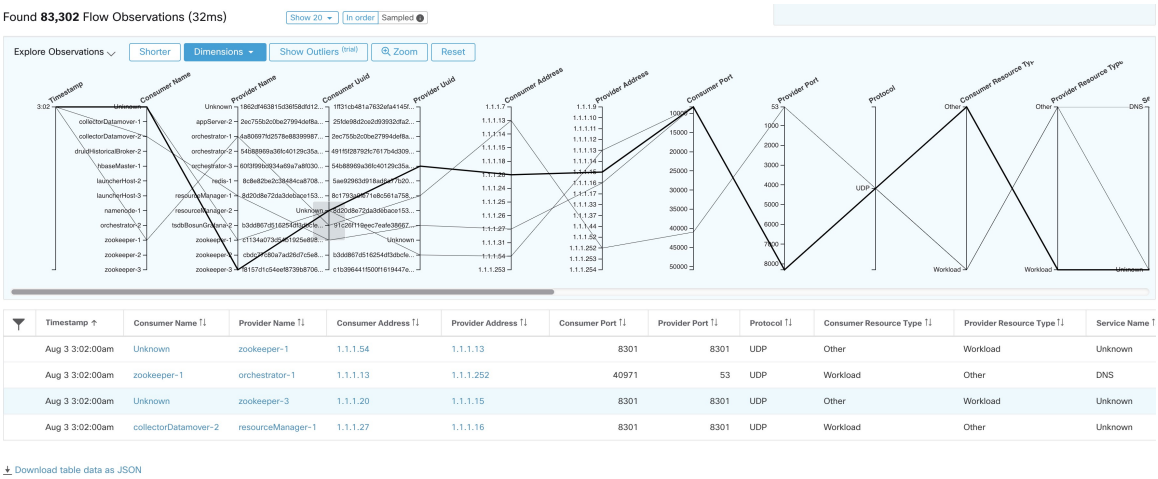
Explorer les observations

Figure 378: Explorer les observations



Cliquez sur **Explore Observations** (explorer les observations) pour activer un affichage graphique permettant d'explorer rapidement les données dont les dimensions sont élevées **(graphique à coordonnées parallèles**). Un peu impressionnant au premier abord, ce tableau est utile pour activer uniquement les dimensions qui vous intéressent (en décochant les éléments du menu déroulant **Dimensions**) et pour réorganiser l'ordre des dimensions. Une seule ligne dans ce graphique représente une seule observation et l'intersection de cette ligne avec les différents axes indique la valeur de cette observation pour cette dimension. Cela devient plus clair lorsque l'on passe le curseur sur la liste des observations sous le graphique pour voir la ligne en surbrillance représentant l'observation dans le graphique :

Figure 379: Observation de flux survolée par le curseur



En raison de la nature complexe des données de flux, ce graphique est large par défaut et nécessite de le faire défiler vers la droite pour le voir en entier. C'est pourquoi il est utile de désactiver toutes les dimensions sauf celles qui vous intéressent.

Par échantillonnage ou par ordre

Il est recommandé d'effectuer les observations Explore avec **l'échantillonnage** activé et avec un plus grand nombre de flux. Cela vous permet de mieux voir la variété des flux qui composent l'intervalle sélectionné. Ainsi, si vous avez sélectionné 2 millions d'observations de flux dans le tableau de séries chronologiques ci-dessus, le chargement d'un échantillon de 1000 flux les choisira uniformément tout au long de l'intervalle, tandis que le chargement des flux **dans l'ordre** chargera les 1000 premières observations de flux depuis le tout début de intervalle :

Figure 380: 1000 par ordre

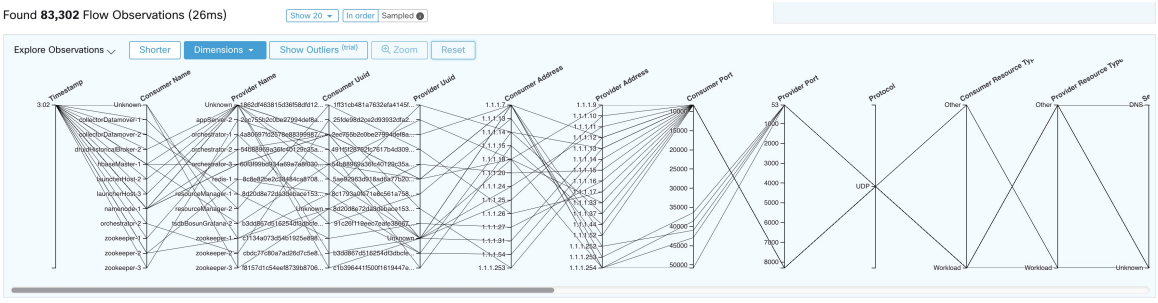
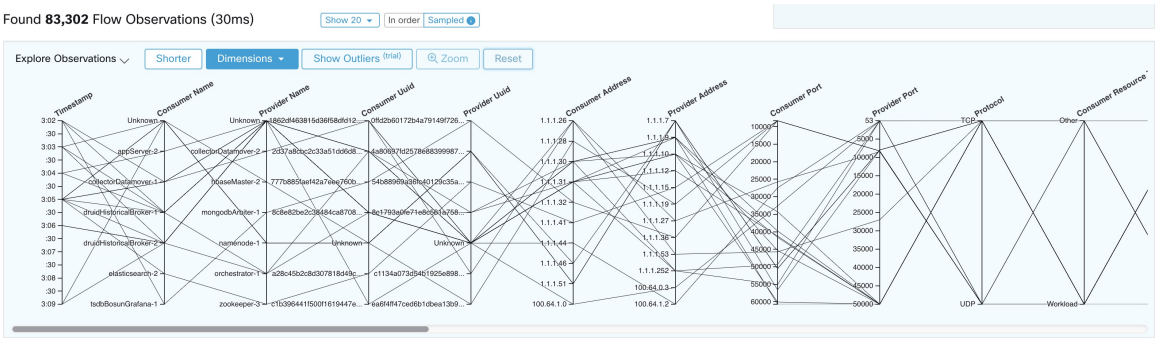


Figure 381: par rapport à 1000 échantillons

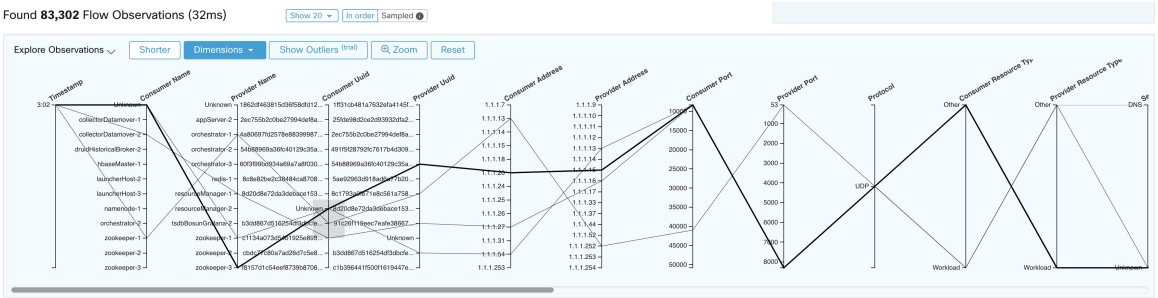


Remarquez que l' **horodatage** de toutes les observations dans l'ordre est 9:09 et que les observations sont réparties uniformément dans l'intervalle sélectionné dans la version échantillonnée.

Filtrage

Faites glisser le curseur le long de l'un des axes pour créer une sélection qui affiche uniquement les observations correspondant à cette sélection. Cliquez à nouveau sur l'axe pour supprimer la sélection à tout moment. Des sélections peuvent être effectuées sur n'importe quel nombre d'axes à la fois. La liste des observations est mise à jour pour afficher uniquement les observations sélectionnées :

Figure 382: Explorer avec sélection



Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 3:02:00am	Unknown	zookeeper-1	1.1.1.54	1.1.1.13	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	zookeeper-1	orchestrator-1	1.1.1.13	1.1.1.252	40971	53	UDP	Workload	Other	DNS
Aug 3 3:02:00am	Unknown	zookeeper-3	1.1.1.20	1.1.1.15	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	collectorDatamover-2	resourceManager-1	1.1.1.27	1.1.1.16	8301	8301	UDP	Workload	Other	Unknown

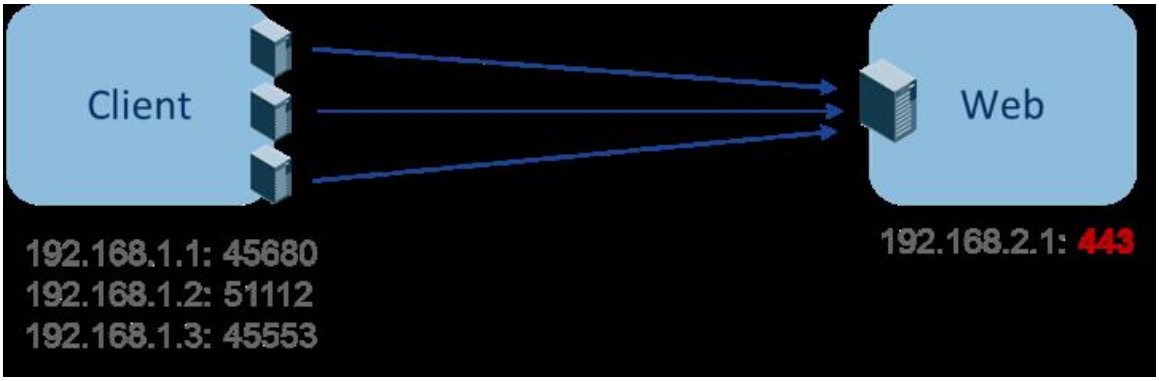
Download table data as JSON

Classification client-serveur

Le sens du flux (classification client/serveur ou fournisseur/consommateur) est important pour la visibilité, la découverte automatique et l'application des politiques. Chaque flux de monodiffusion comporte une classification client et une classification serveur.

Par exemple, si des clients (192.168.1.1-192.168.1.3) accèdent à un serveur Web (192.168.2.1) à l'aide de https, le port source est généralement un port éphémère dans la plage 1025-65535 et le port de destination est 443.

Figure 383: Classification client-serveur



La direction précise client-serveur est :

- Client : 192.168.1.1-3
- Serveur : 192.168.2.1
- Services : Port TCP 443

Les politiques générées par la découverte automatique des politiques sont indiquées dans la figure (avec les points terminaux de gauche regroupés) :

Figure 384: Politiques générées

Maintenant, si la décision dans le sens client-serveur est inversée (une classification inexacte), l'on trouve :

- Client : 192.168.2.1
- Serveur : 192.168.1.1-3
- Services : la liste des ports éphémères (45680, 51112, 45553)

Ensuite, dans la classification inexacte ci-dessus, les politiques générées peuvent être celles indiquées dans la figure :

Figure 385: Classification inexacte

Cela consomme plus de ressources en termes d'application des politiques. En outre, selon la façon dont vous appliquez la politique, même si 192.168.1.1-3 utilise ces ports éphémères, ils ne peuvent pas accéder à 192.168.2.1. Par exemple, si vous utilisez Cisco Secure Workload, la mise en application des capteurs logiciels, la politique d'application pour la condition Client vers le Web ci-dessus (ESTAB) ne correspond pas au trafic généré par le client destiné au Web (NEW, ESTAB).

Les horodatages et les indicateurs TCP sont utilisés dans Cisco Secure Workload pour déterminer le sens client-serveur. S'il n'y a aucune information d'indicateurs TCP (SYN, SYN/ACK) parce que, par exemple, les paquets peuvent être UDP/ICMP ou parce qu'un capteur matériel ne prend pas en charge les signaux de direction, les règles de remplacement définies par l'utilisateur, les horodatages et autres méthodes empiriques sont utilisés pour déduire la direction du flux. Par définition, les méthodes empiriques ne garantissent pas une précision à 100 %. La précision client-serveur est fonction du type de capteur utilisé et des conditions dans lesquelles les capteurs sont utilisés. Vous pouvez utiliser l'API REST (OpenAPI) de Cisco Secure Workload pour insérer des règles de remplacement client-serveur afin d'identifier les ports de serveur pour les types de flux qui font que Cisco Secure Workload se trompe de direction. Autorisez ensuite Cisco Secure Workload à traiter les nouveaux flux de données captés avec ces règles en place, puis générez les politiques sur la durée lorsque la direction du flux a été déterminée. Pour plus de détails sur l'API pour spécifier les règles de remplacement, consultez : Configuration client-serveur, on page 1062. Vous pouvez également définir manuellement les politiques et examiner/supprimer les politiques indésirables. Consultez Politiques, on page 954.

Recommandation de type de capteur

Une visibilité approfondie ou les agents logiciels d'application fournissent les meilleurs signaux aux algorithmes de classification client-serveur Cisco Secure Workload. Nous sommes invités à envisager de déployer des agents d'application ou de visibilité approfondie. Ces agents reçoivent tous les signaux nécessaires pour établir une classification client-serveur correcte. Si le déploiement d'agents d'application ou de visibilité approfondie n'est pas possible pour certaines charges de travail, il est recommandé d'utiliser les capteurs ERSPAN et de s'arrêter là pour la découverte automatique des politiques. Cisco Secure Workload nous aide du mieux possible et nous améliorons continuellement nos algorithmes heuristiques en fonction des commentaires.

Lorsque les informations correctes sur la direction client-serveur ne sont pas disponibles, Cisco Secure Workload utilise des dérogations définies par l'utilisateur ou une heuristique pour déduire la direction. Par définition, les méthodes empiriques ne garantissent pas une précision à 100 %. La précision diminue avec le type de capteur utilisé et les conditions dans lesquelles il a été utilisé.

Le tableau suivant est l'ordre recommandé pour la décision client-serveur dans les scénarios de génération de politiques :

- **Agents de visibilité approfondie ou d'application** : pour de meilleurs résultats, utilisez des capteurs logiciels (agents de visibilité approfondie ou d'application). Les flux de trafic ayant commencé avant le démarrage du capteur seront traités par une méthode heuristique qui est abordée ci-dessous.

- Les capteurs ADC de **comme F5/Citrix/. . . agents** : ces agents recueillent l'état client-serveur des périphériques ADC et diffusent cette source fiable dans Cisco Secure Workload.
- **Capteurs ERSPAN** : avec un capteur ERSPAN, l'utilisateur doit veiller à fournir une visibilité complète du trafic à destination et en provenance de la charge de travail concernée et s'assurer que le capteur ERSPAN voit tout le trafic réparti. Le capteur ERSPAN ne doit pas non plus être trop sollicité, de sorte que sa visibilité ne soit pas affectée par la communication réseau de la charge de travail. En outre, l'utilisateur doit s'assurer que les pertes de paquets des capteurs ERSPAN sont réduites au minimum. L'opérateur ne verra pas les informations de processus avec les informations de flux de réseau pour la découverte automatique des politiques.

En utilisant le capteur Netflow énuméré ci-dessous, l'utilisateur doit s'engager dans un travail manuel beaucoup plus important pour l'analyse de la politique et la génération de règles d'exception. Cisco Secure Workload utilise largement la méthode heuristique, qui, par définition, n'est pas précise à 100 %.

- **Capteur** NetFlow : NetFlow fournit des données de flux échantillonnées et agrégées. Les processus d'agrégation et d'échantillonnage provoquent la perte d'informations sur la direction client-serveur. Cela a une incidence sur les résultats de la découverte automatique des politiques et de la génération de ces dernières et rend le problème plus ardu. Les données NetFlow sont excellentes pour une visibilité globale. Cisco Secure Workloaddoit se rabattre sur l'heuristique qui, si elle est incorrecte, exige parfois davantage de travail manuel de la part de l'opérateur - comme la définition de règles d'exception pour la charge de travail sécurisée. Les données NetFlow omettent également certains des flux courts et la qualité du signal dépend du périphérique qui produit les données NetFlow. Nous vous recommandons d'utiliser NetFlow avec Cisco Secure Workload pour les cas d'utilisation spécialisés comme l'assemblage des flux à travers des périphériques NAT L3/L4 comme dans le cas des contrôleurs de livraison d'application (ou des équilibreurs de charge de serveur) pour fournir à Cisco Secure Workload la visibilité de quel flux est lié à quel autre flux.

L'analyse de la direction client-serveur est décrite plus en détail ci-après.

Identification des producteurs (serveurs) et des consommateurs (clients) d'un flux

Il existe plusieurs façons (souvent pragmatiques) de détecter les serveurs :

- Si un capteur constate l'établissement de liaison SYN, il peut déterminer qui est le serveur.
- Basée sur le temps : l'initiateur d'une connexion est considéré comme un client.
- Modèle du degré : généralement, de nombreux clients communiquent avec un serveur. En revanche, le degré du port client devrait être largement inférieur.

L'ordre de priorité est SYN_ANALYSIS/NETSTAT > USER_CONFIG > DEGREE_MODEL.

Le raisonnement qui consiste à donner à SYN_ANALYSIS une priorité plus élevée que la configuration de l'utilisateur est que la configuration peut être périmée et que le capteur a le meilleur point d'observation pour établir la réalité du terrain. DEGREE_MODEL est l'endroit où l'apprentissage et les méthodes heuristiques entrent en jeu, et la précision ne peut pas être garantie à 100 %.

Il est possible que notre approche heuristique de la détection client-serveur soit erronée, malgré nos meilleures intentions et les améliorations algorithmiques constantes que nous apportons dans ce domaine. Dans ces scénarios, l'interface OpenAPI peut être utilisée pour marquer les ports de serveur bien connus. Ces configurations ne sont pas appliquées aux flux passés et n'affectent que les marquages des flux à partir du

moment présent (c'est-à-dire les flux suivants). Il s'agit d'une solution de repli de dernier recours, plutôt que le mode de fonctionnement normal.

Nous recommandons également de ne pas continuer à intervertir le marquage client-serveur pendant toute la durée d'un flux donné (même si nous nous trompons et si nos modèles internes ont changé - ce qu'ils font au fil du temps, à mesure que de nouveaux modèles de flux sont observés ou analysés). Les mises à jour de priorité supérieure ou égale sont autorisées à remplacer celles de priorité inférieure (nous inverserons également le serveur client pour les flux existants). En d'autres termes, la régularité de la correction « pour la durée de vie d'un flux » ne s'applique qu'à la correction basée sur un modèle de degré.

Conversation Mode

By default, the flow analysis fidelity mode in agents is "detailed". Historically, this was the only mode available, where, every observed flow was reported by the agent along with detailed stats about the observed flow. Stats like: packet and byte counts, TCP flags, connection stats, network latency, srtt, etc.

While this kind of reporting is desirable in a lot of cases, it is computationally intensive to report and process, also, it may not be strictly required when the primary use case is segmentation only.

The **Conversation Mode** offers a more lightweight alternative to the traditional detailed mode. Agents in conversation mode aim to report conversations as opposed to flows whenever possible (i.e, whenever they are able to make the client-server classification accurately). This is applicable to TCP, UDP and ICMP flows.

In detailed mode, for TCP/UDP flows, we report 5-tuple flows {source and destination IP, source and destination port, and protocol}.

While for conversation mode, agent omits the source port as they are ephemeral ports {changes on every new connection}, making it a 4-tuple flow.

Note Detecting a flow as 4-tuple also depends on client server detection algorithms, which relies on server/destination port being a well-known port (0 through 1023) .

Thus, if you are using a custom application which does not use well-known server/destination ports, the OpenAPI interface can be used to punch well known server ports. These configs are not applied to past flows, and only affect markings on flows from that point on (i.e., going forward). To optimize server ports, see Client Server Configuration.

Agent reports in conversation mode contain trimmed down information, full list of omitted fields includes: TCP/UDP source port (ephemeral ports), Fwd/Rev TCP bottleneck, TCP handshake bucket, SRTT(µs), Fwd/Rev Packet retransmissions, SRTT Available, Fwd/Rev Congestion Window Reduced, Fwd/Rev MSS Changed, Fwd/Rev TCP Rcv Window Zero?, Fwd/Rev Burst Indicator, Fwd/Rev Max Burst Size (KB).

To enable conversation mode, please refer to the Flow Visibility config section in: Configuration de l'agent logiciel

Note The exact benefit gained by changing agents to report in conversation mode may vary due to multiple factors, including, but not limited to percentage of TCP flows, number of services listening on well known service ports, and memory limitations at the agent.

Note After turning on “conversation” mode for some agents, there may be a mixture of conversations and flows in the observations on the flow search page.

Visibilité dans les flux mandatés

Un serveur mandataire agit comme un serveur placé entre les ordinateurs clients et Internet, contrôlant et restreignant l’accès direct du client à Internet. Lorsqu’un client souhaite accéder aux services Internet, il ordonne au serveur mandataire d’établir une connexion TCP avec les serveurs Web en son nom. Après avoir établi la connexion avec succès, le serveur mandataire envoie une réponse HTTP avec un état au client. Ultérieurement, le client interagit sur la connexion TCP établie, semblant communiquer directement avec le service Web. Le serveur mandataire sert de pont, ce qui facilite la transmission des données entre les deux connexions TCP.

La charge de travail, qui héberge une application sur laquelle l’agent CSW est installé, lance une demande de services Internet. Au départ, il demande au serveur mandataire de créer un canal de communication en son nom. L’interaction avec le service Internet a lieu via la connexion établie avec le serveur mandataire. L’agent CSW capture uniquement le flux entre la charge de travail et le serveur mandataire. La destination réelle de ce flux reste inconnue avec la configuration actuelle de l’agent CSW.

L’agent utilise le filtre pcap actuel pour analyser tous les paquets TCP sortants, à la recherche du Verbe HTTP « CONNECT » dans la charge utile. Ce processus permet à l’agent de capter la demande de serveur mandataire dans le flux. Lors de l’exportation des flux vers les collecteurs, l’agent génère un **flux effectif** pour chaque flux de serveur mandataire identifié. Il établit une connexion entre le serveur mandataire et les flux soumis à un mandataire à l’aide du champ **related_key** (clé liée) en incorporant les informations sur les quintuples.

Note Cette fonction est activée par défaut. Pour la désactiver, ajoutez *Enable_serveur mandataire_flows_visibility: 0* au fichier de configuration du capteur.

Préalables

Régler la fidélité de l’analyse de flux sur Mode détaillé.

Note

- Fonctionne uniquement avec un serveur mandataire HTTP/HTTPS.
- Capture uniquement les demandes CONNECT. Actuellement, les demandes GET ne sont pas prises en charge.
- Par défaut, le mode de fidélité pour l’analyse de flux des agents est **Conversations**.

Procédure

1. Dans le menu de navigation choisissez **Investigate** > **Traffic** (Enquêter sur le trafic).

   Cette page facilite le filtrage rapide et l’exploration en profondeur du corps de flux.

2. Développez-la pour afficher les détails du flux.

Les agents dans la version 3.9 ou ultérieure peuvent capturer la destination des flux par serveur mandataire. À la page **Investigate** > **Traffic**, vous pouvez observer les deux flux distincts :

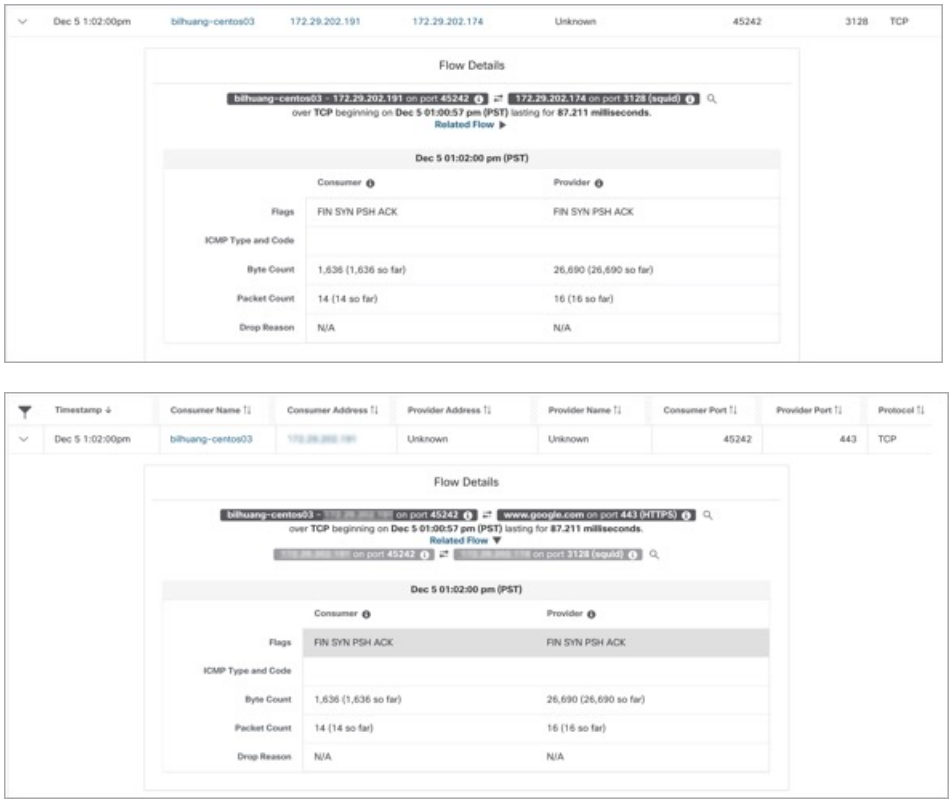
a. **Flux de serveur mandataire** : provenant de la charge de travail vers le serveur mandataire.

b. **Flux mandataire** : représentant un flux effectif et canalisé depuis la charge de travail jusqu'au nom de domaine complet (FQDN) ou l'adresse distante.

Ces flux sont interconnectés et désignés comme **Associés**. Les considérations spécifiques sont les suivantes :

- Si la demande au serveur mandataire est dirigée vers un nom de domaine complet distant, l'**adresse du fournisseur** du flux effectif est marquée comme **Unknown** (Inconnue), mais le **nom de domaine du fournisseur** est défini sur le nom de domaine complet.
- Si la demande au serveur mandataire est dirigée vers une adresse IP distante, l'adresse du **fournisseur** est cette adresse spécifique, tandis que le **nom de domaine du fournisseur** est laissé vide.

Figure 386: Détails des flux



CHAPITRE 10

Configurer les alertes

Les alertes de Cisco Secure Workload vous aident à surveiller la sécurité de la charge de travail et à réagir aux menaces potentielles. Les différents composants des alertes fonctionnent ensemble pour fournir une visibilité, les sources et configuration des alertes, et la capacité d'envoyer des alertes à partir des serveurs de publication d'alertes. Vous pouvez configurer des alertes, afficher les règles de leur déclencheur et choisir les serveurs de publication d'alertes à qui les envoyer. Les alertes affichées sur la page de configuration varient selon le rôle de l'utilisateur. Les serveurs de publication d'alertes peuvent être des alertes ou des notificateurs.

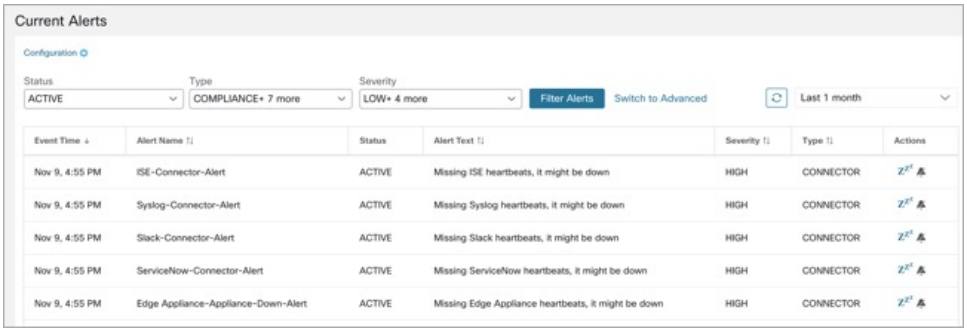
Remarque À partir de la version Secure Workload 3.0, l' Cisco Secure WorkloadApp Store ne prend pas en charge les applications d'alertes et de conformité. Vous pouvez configurer des alertes et des alertes de conformité sur cette page sans créer d'instance d'application d'alerte ou d'application de conformité.

Types d'alertes et serveurs de publication

Les alertes Cisco Secure Workload se composent des éléments suivants :

1. **Visibilité des alertes :**
   - **Alertes actuelles**: dans le volet de navigation, choisissez **Investigate (Investiguer)** > **Alerts (Alertes).** Un aperçu des alertes est envoyé à un surveilleur de données.

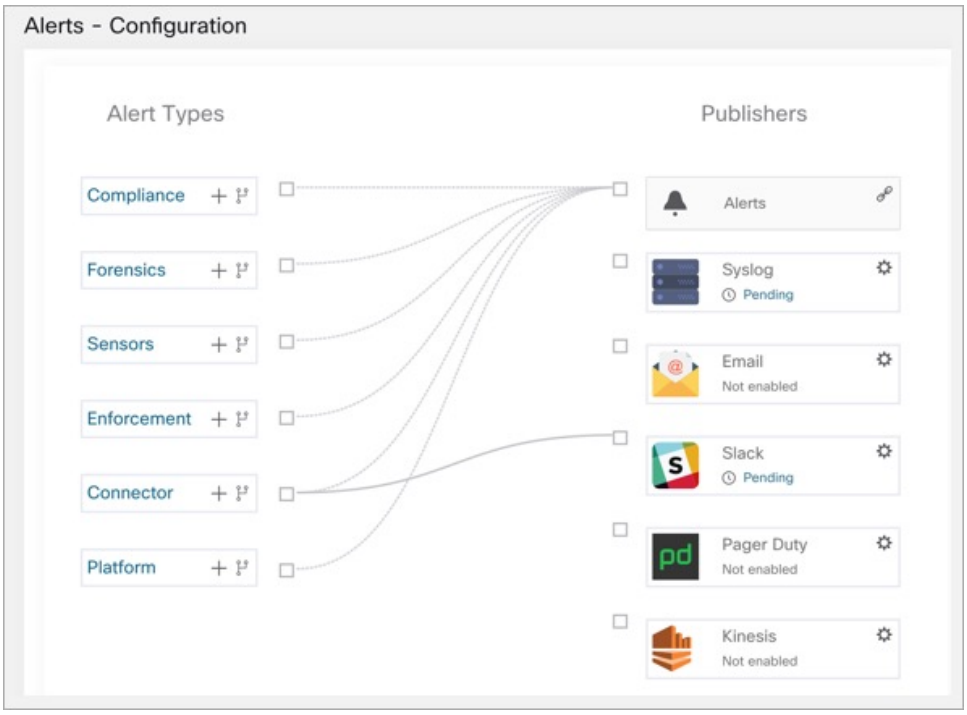
Figure 387: Alertes actuelles



2. **Source et configuration des alertes**

   - **Alertes-Configuration** : Accédez à **Manage (Gestion)** > **Alerts Configs (Configuration des alertes)** . Les configurations d'alertes qui sont configurées à l'aide du serveur de publication modal et d'alertes commun et les paramètres de l'émetteur de notifications sont affichées.

Figure 388: Alertes - Configuration



3. **Envoyer des alertes**

   - **Application Alerts** : une application Cisco Secure Workload implicite qui envoie les alertes générées à un surveilleur de données configuré. L'application Alerts gère des fonctionnalités telles que la **répétition** et la **sourdine**.

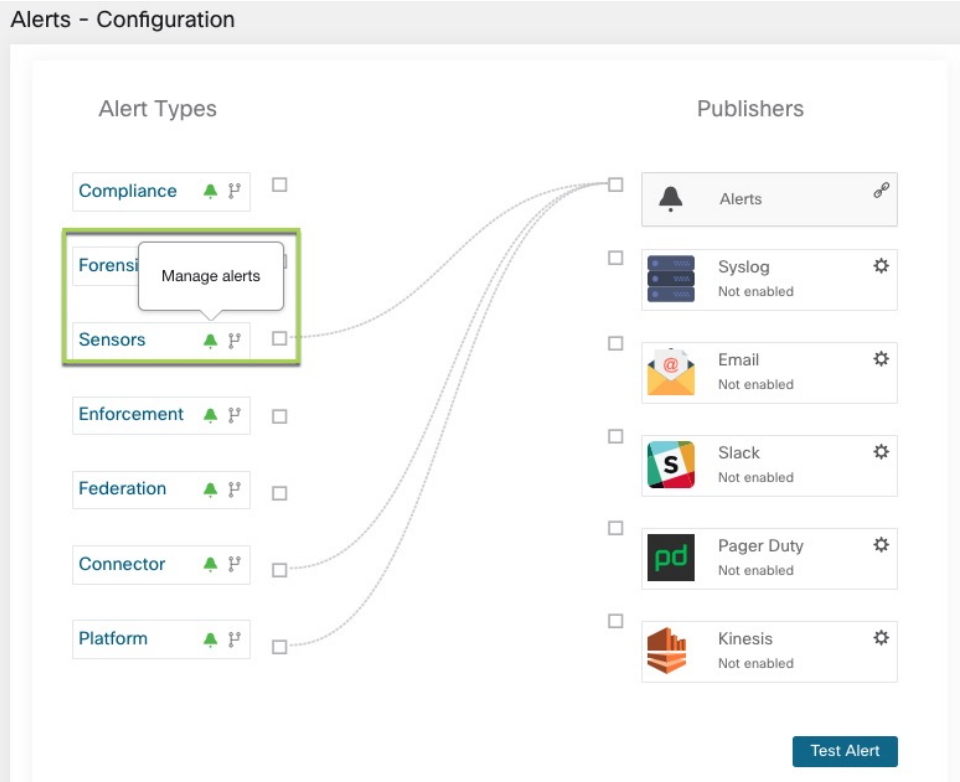
   - **Serveur de publication d'alertes** : limite le nombre d'alertes affichées et envoie les alertes à Kafka (MDT ou surveilleur de données Data Tap) pour utilisation externe.

- **Appareil de périphérie** : envoie des alertes à d'autres systèmes comme Slack, PagerDuty, Courriel, etc.

Créer des alertes

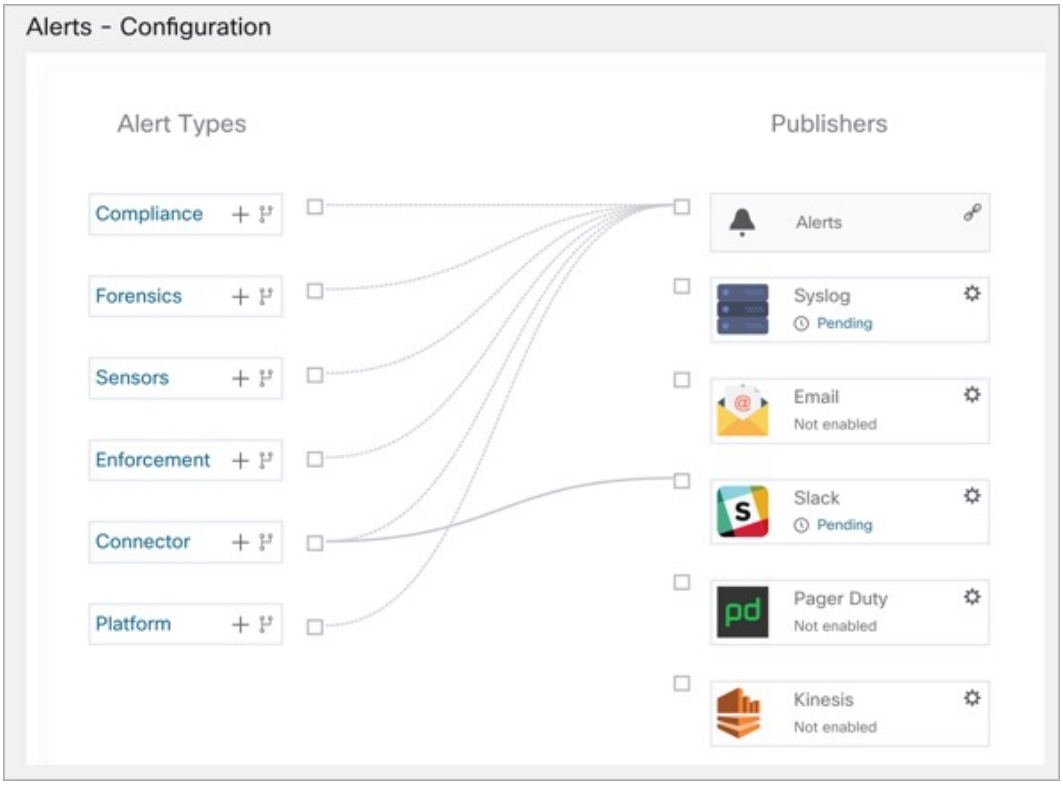
Dans le volet de navigation, choisissez **Alerts** > **Configuration** (configuration des alertes) pour créer des alertes :

Figure 389: Créer une alerte (règle de déclenchement)



Dans le volet de navigation, choisissez **Alerts (Alertes)** > **Configuration(Configuration)** pour configurer les types d'alertes suivants :

Figure 390: Créer une alerte



- **Alertes de mise en application**
  - Accessibilité de l'agent
  - Pare-feu de charge de travail
  - Politique de charge de travail
- **Alertes de capteurs**
  - Mise à niveau de l’agent
  - Exportation du flux de l’agent
  - Connection de l'agent
  - Utilisation de la mémoire de l’agent
  - Quota de CPU (processeur) de l’agent
  - Quantité d’observations de flux
  - Nouvel agent enregistré
  - État Pcap
  - Agent désinstallé
  - Chiffrement non recommandé

- Version TLS obsolète
- Suppression automatique de l'agent

- **Alertes de conformité**
  - Politique de mise en application
  - Politique d'analyse en direct

Note

- Les règles de déclencheur d'alerte sont appliquées à la portée racine actuellement sélectionnée pour les types d'alertes Enforcement (Application) et Sensors (Capteurs).
- Vous devez avoir une capacité appliquée sur la portée actuellement sélectionnée pour créer une règle de déclencheur d'alerte pour le type d'alerte de conformité.

Les types d'alertes suivants ne possèdent pas de boîte de dialogue modale de configuration :

- Alertes criminalistiques
- Alertes du connecteur
- Fédération
- amiral

Boîte de dialogue modale de configuration des alertes

La boîte de dialogue modale de configuration d'alerte se compose des sections suivantes :

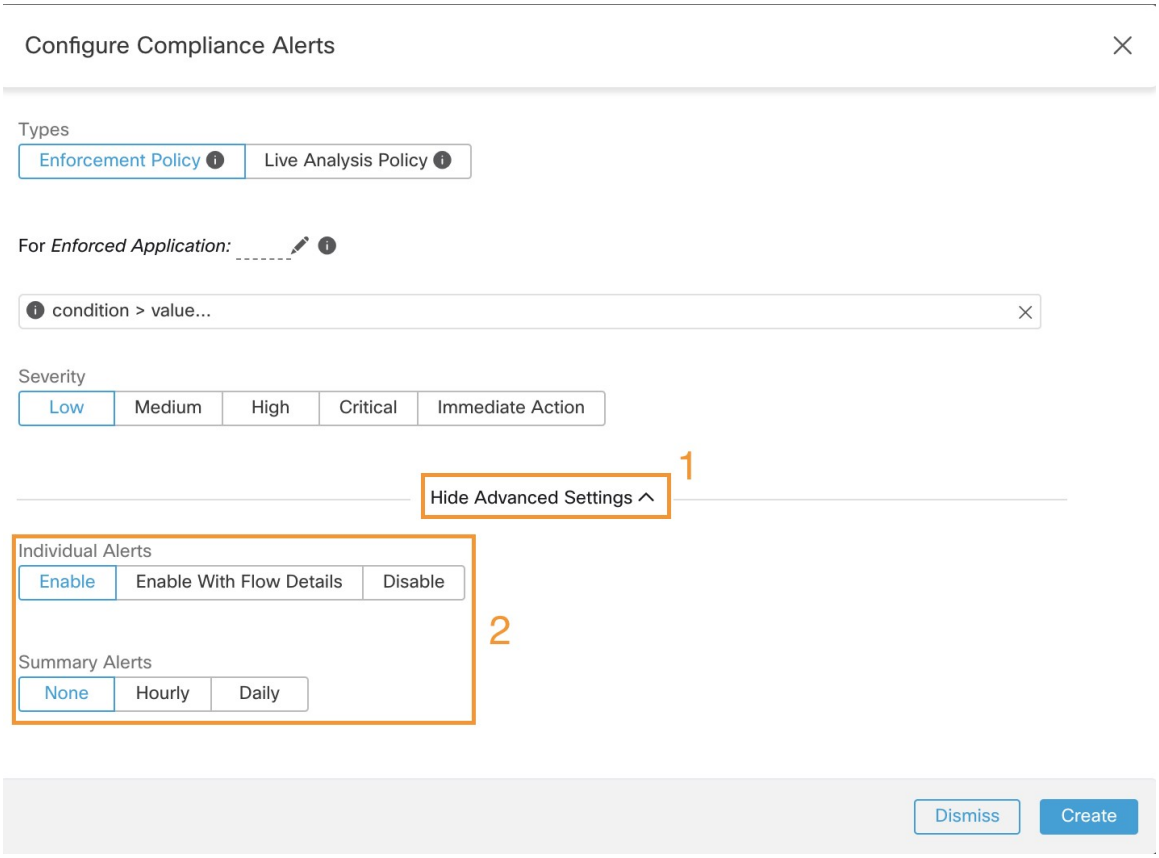
- Les types d'alertes sont affichés lorsque la configuration de l'alerte varie selon le *l'objet*

Note Les types d'alertes pour les alertes de voisinage ne sont pas disponibles pour Cisco Secure Workload 3.7 et les versions antérieures.

- L' *objet* de l'alerte. L'objet dépend de l'application et peut être prérempli lorsque la boîte de dialogue modale de l'alerte est contextuelle.
- Déclenchement d'une alerte : *« quand allons-nous générer une alerte »*. Passez le curseur sur l'icône pour trouver une liste des conditions disponibles. La liste affiche les conditions disponibles spécifiques au type d'alerte pour la configuration.
- Gravité des alertes : si de nombreuses alertes sont générées, les alertes de gravité plus élevée sont affichées de préférence par rapport aux alertes de gravité inférieure.
- les options de configuration pour les options d'alerte résumées. Cliquez sur **Show Advanced Settings (afficher les paramètres avancés)** pour les développer.

- Fermer la boîte de dialogue : utilisez **Create** (Créer) si vous ajoutez une nouvelle alerte avec toutes les options de configuration spécifiées ou **Dismiss** (Rejeter) si vous n'ajoutez pas de nouvelle alerte.

Figure 391: Options avancées de la boîte de dialogue modale de configuration des alertes

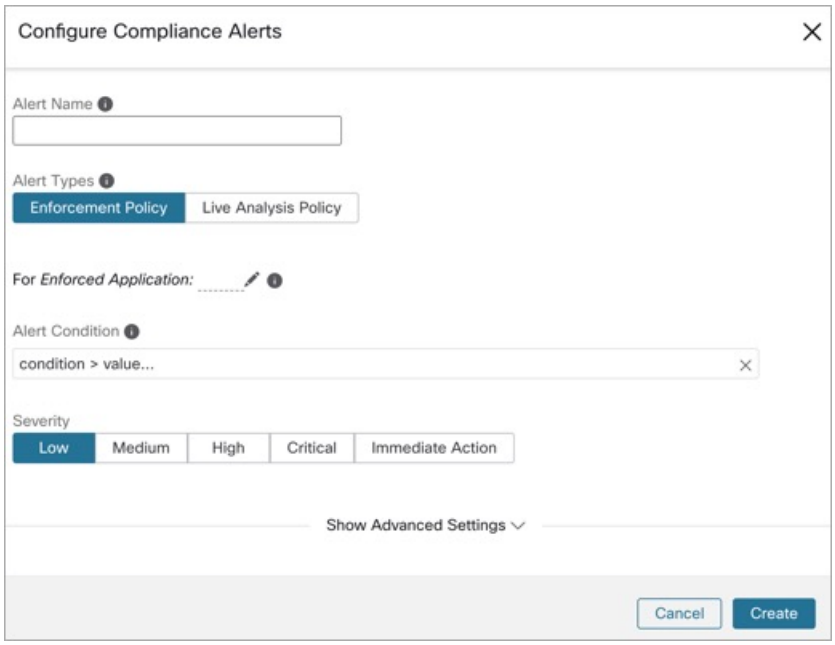


- Le **nom de l'alerte**.
- Les **Types d'alertes**
- Le *sujet* d'une alerte. L'objet dépend de l'application et peut être prérempli lorsque la boîte de dialogue modale de l'alerte est contextuelle.
- La **condition d'alerte** pour laquelle une alerte est déclenchée. Passez le curseur sur l'icône d' **information** pour afficher une liste des conditions disponibles.
- Si plusieurs alertes sont générées, les alertes avec une *gravité* plus élevée sont affichées de préférence par rapport aux alertes avec une gravité plus faible.
- Cliquez sur **Show Advanced Settings** (afficher les paramètres avancés) pour accéder à plus d'options de configuration.

Note

- À la fin de la mise à niveau, toutes les règles de configuration d'alertes existantes des détenteurs actuels reçoivent un **nom d'alerte** selon le format prédéfini. Dans les cas où le nom de l'alerte est absent, le format à utiliser est *Alert_SubType_{DatabaseID}*. Par exemple, Workload_Firewall_64bf9b8493dfc94ca0095718.
- Après le déploiement ou la mise à niveau, toutes les règles de configuration d'alerte par défaut (celles qui sont créées lors de la création d'un nouveau détenteur) se voient attribuer un **nom d'alerte** au format prédéfini : *Alert_SubType*. Par exemple, État_Mise à niveau.

Figure 392: Configurer les alertes



Alertes résumées

Les alertes résumées sont autorisées pour certaines applications et les options de configuration dépendent de l'application.

- Par **alertes individuelles**, on entend les alertes générées à partir d'informations non agrégées (ou faiblement agrégées) et qui sont susceptibles de durer une minute. Notez que cela ne signifie pas nécessairement que les alertes sont réellement générées et envoyées à une minute d'intervalle; les alertes individuelles peuvent toujours être générées à l'intervalle de *fréquence de l'application*.
- **Ls alertes résumées** se réfère aux alertes générées sur des métriques produites pendant une heure ou à la synthèse d'alertes moins fréquentes.

Application	Fréquence de l'application 1	Alertes individuelles	Alertes toutes les heures	Alertes quotidiennes
Conformité	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel
Exécution	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel
Capteurs	Minute	Oui : à la fréquence de l'application	Résumé individuel	Résumé individuel

Note L'heure de l'événement des alertes résumées représente la première occurrence d'une alerte du même type au cours de la dernière heure ou au cours d'une fenêtre d'intervalle donnée.

Remarque sur la récapitulation par rapport à la répétition d'alarme

La récapitulation s'applique à l'ensemble complet des alertes générées selon la configuration des alertes, tandis que la répétition d'alerte s'applique à une alerte spécifique. Cette distinction est mineure lorsque la configuration d'alerte est très spécifique, mais elle est notable lorsqu'elle est large.

- Par exemple, la configuration de la conformité est assez large : elle porte sur un espace de travail d'application et sur le type de violation pour lequel une alerte doit être générée. Ainsi, la récapitulation s'appliquerait à toutes les alertes déclenchées par une condition « escaped (échappé) », tandis que la répétition s'appliquerait à une portée de consommateur, à une portée de fournisseur, à un port de fournisseur, à un protocole et à la condition échappée très spécifiques.
- À l'opposé, une alerte de plateforme configurée pour envoyer une alerte sur un chemin entre la portée source et la portée de destination avec un nombre de sauts inférieur à une certaine quantité générera une alerte très spécifique.

Autres distinctions

- La répétition d'une alerte n'entraîne son envoi que lorsqu'une nouvelle alerte est générée après l'expiration de l'intervalle de répétition. Rien n'indique le nombre d'alertes supprimées qui auraient pu se produire pendant l'intervalle de répétition.
- Un résumé d'alerte est généré à une fréquence donnée, quel que soit le nombre d'alertes ont générées au cours de cet intervalle. Les résumés d'alertes indiquent le nombre d'alertes déclenchées au cours de la période, ainsi que des mesures agrégées ou par plages.

Outil de notification d'alertes Cisco Secure Workload (TAN)

Note À partir de la version 3.3.1.x de Cisco Secure Workload, le TAN est déplacé vers **l'appareil Cisco Secure Workload de périphérie**.

Les émetteurs de notifications offrent des fonctionnalités pour envoyer des alertes par l'intermédiaire de divers outils tels qu'Amazon Kinesis, Email, Syslog et Slack dans la portée actuellement sélectionnée. En tant que propriétaire de la portée ou administrateur du site, chaque notificateur peut être configuré avec les informations d'authentification requises et d'autres informations spécifiques à l'application du notificateur.

Configurer les outils de notification

Pour configurer des notificateurs, vous devez configurer les connecteurs liés aux alertes. Les connecteurs ne peuvent être configurés qu'après le déploiement d'un appareil de périphérie Cisco Secure Workload. Pour de plus amples renseignements sur le déploiement d'un appareil de périphérie Cisco Secure Workload, consultez Appliances virtuelles pour les connecteurs.

Une fois que l'appareil de périphérie Cisco Secure Workload est configuré, vous pouvez configurer chaque émetteur de notification avec l'entrée requise spécifique. Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pourrez voir des lignes pointillées connecter les types d'alertes au serveur de publication d'alertes. En effet, l'outil de notification repose sur le serveur de publication d'alertes.

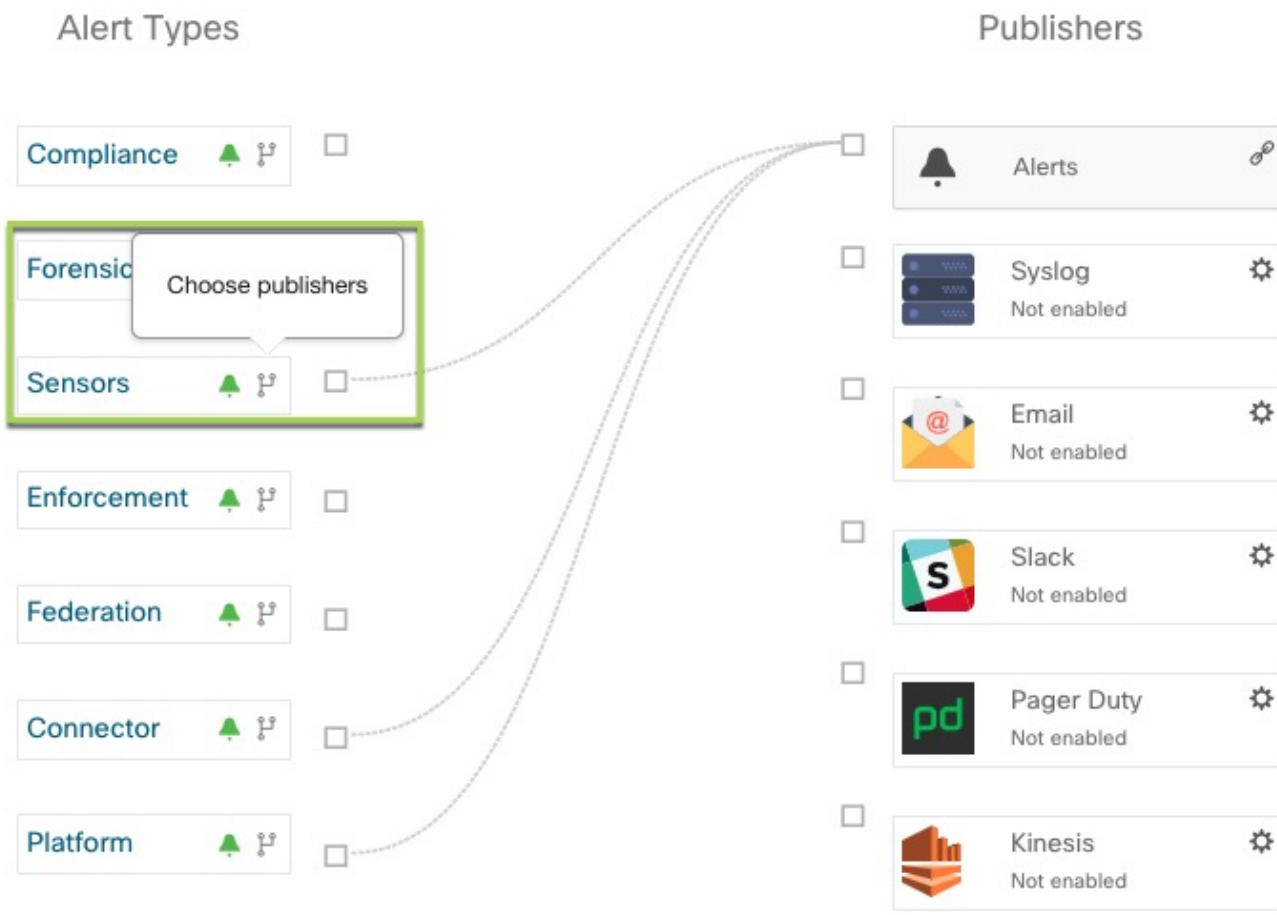
Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pouvez configurer chaque notificateur avec l'entrée requise. Une fois l'appareil de périphérie Cisco Secure Workload configuré, vous pouvez afficher les lignes en pointillés reliant les types d'alertes au serveur de publication. Cela est dû au fait que l'outil de notification est construit sur le serveur de publication.

La fréquence de l'application est environ la fréquence à laquelle l'application s'exécute et génère des alertes. Par exemple, le service de conformité a une fréquence d'exécution flexible et peut en fait calculer les alertes sur quelques minutes.

Choisir les serveurs de publication d'alertes

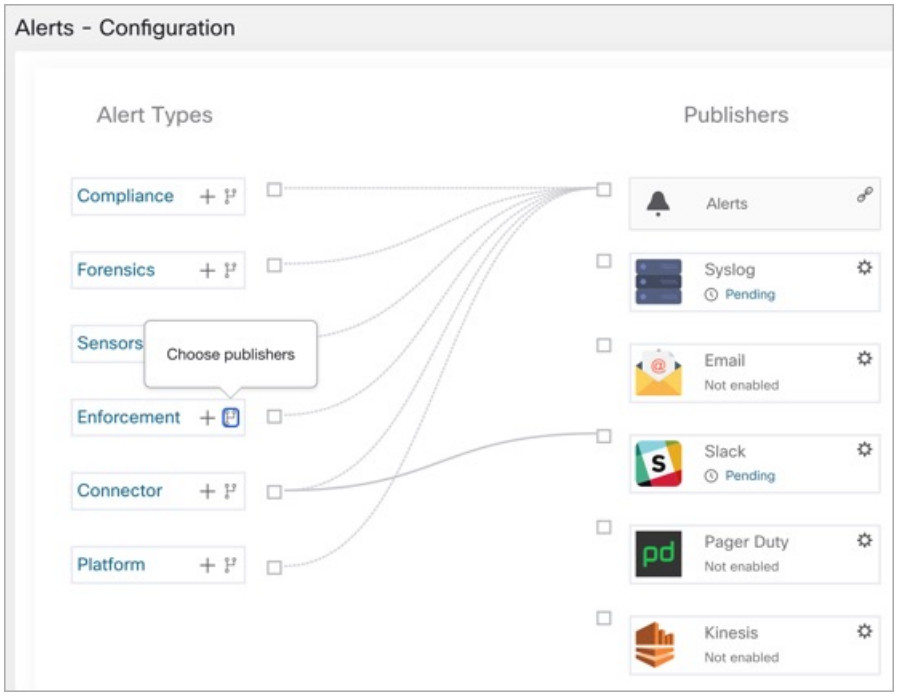
Les propriétaires de la portée et les **administrateurs de site** peuvent choisir les serveurs de publication auxquels **envoyer** des alertes. **Les serveurs de publication** incluent Kafka (Data Tap) et les émetteurs de notifications.

Figure 393: Choisir les serveurs de publication d'alertes



Tous les serveurs de publication disponibles sont affichés dans la fenêtre **Alertes - Configuration**, y compris les **alertes** et **les notificateurs actifs**. Vous pouvez activer ou désactiver l'icône **Envoyer** pour choisir les serveurs de publication du type d'alerte. Le niveau de gravité minimal d'alerte fait référence au niveau de gravité qu'une alerte doit atteindre pour être envoyée par l'intermédiaire des serveurs de publication.

Figure 394: Choisir les serveurs de publication d'alertes



Note Le choix des dérivations de données externes peut avoir une incidence sur le nombre maximal d'alertes qui peuvent être traitées; le nombre maximal d'alertes qui peuvent être traitées pourrait être réduit à 14 000 alertes par lot d'une minute.

La tunnellisation Syslog externe est transférée vers le TAN

Note À partir de la version 3.1.1.x, la fonction de tunnellisation syslog est transférée vers le TAN. Pour configurer le journal système afin d'obtenir les événements de journalisation au niveau de la plateforme, vous devez configurer le TAN Cisco Secure Workload sur l'appareil de périphérie dans la portée racine par défaut. Lorsque l'appareil de périphérie Cisco Secure Workload est configuré sur la portée racine par défaut, vous pouvez configurer le serveur syslog. Pour activer les alertes de plateforme, activez les notifications syslog pour la plateforme. Cela peut être fait en activant la connexion Plateforme Syslog.

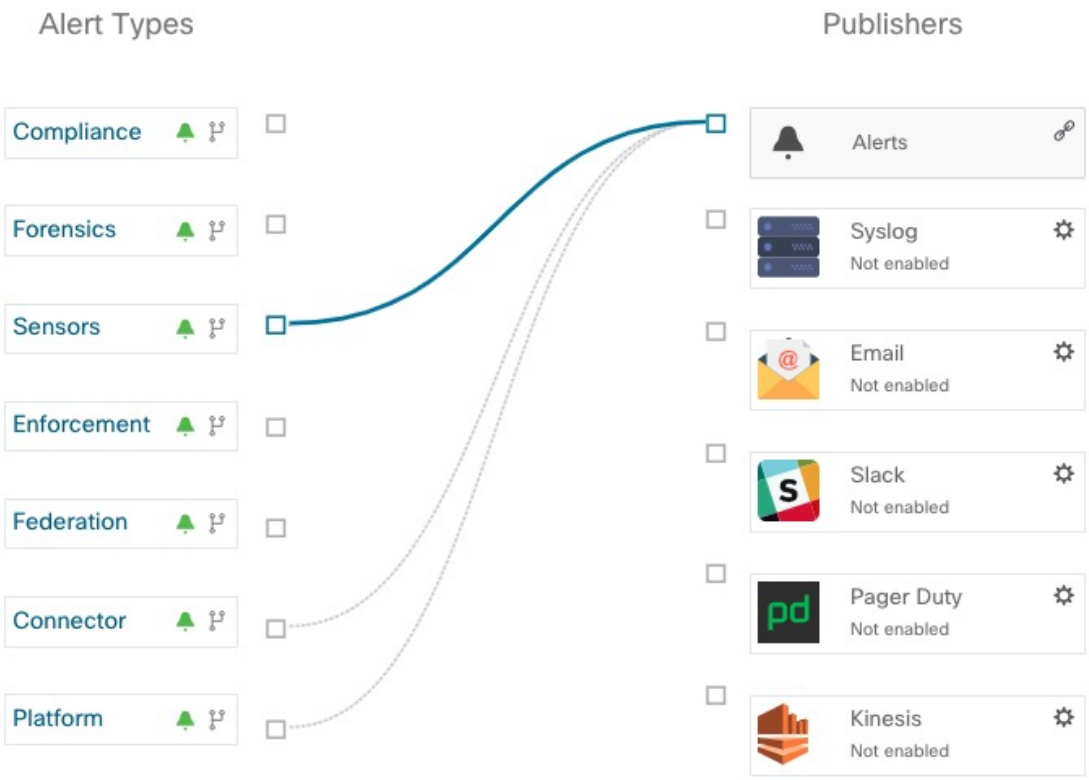
Pour en savoir plus, consultez Connecteur Syslog pour obtenir des détails sur la configuration de syslog.

Tableau des connexions

Le tableau des connexions affiche les liaisons entre **types d'alertes** et **serveurs de publication**. Une fois que vous avez choisi un serveur de publication pour un type d'alerte, une ligne bleue est établie entre le type d'alerte et ce dernier. Notez que la ligne pointant vers le Kafka interne (surveilleur de données) est toujours une ligne pointillée car elle représente un mécanisme interne de mise en œuvre de la notification des alertes.

Figure 395: Tableau des connexions

Figure 396: Tableau des connexions



Note Les alertes générées par l'application utilisateur ne s'affichent pas dans la page de configuration des alertes. Les applications utilisateur peuvent envoyer des messages et des alertes à n'importe quel surveilleur de données (Data Tap) configuré.

Afficher les règles de déclencheur d'alertes

Vous pouvez afficher une liste de toutes les règles de déclenchement d'alertes configurées sur la page **Alertes - Configuration**.

- Vous pouvez filtrer les règles par **type d'alerte** et autres propriétés.
- Dans la colonne **Actions**, cliquez sur l'icône en forme de **crayon** pour modifier les détails comme le nom de l'alerte, les types d'alerte, la condition de l'alerte, la gravité, etc.
- Cliquez sur **See All Configured [alert type] Alerts** (afficher toutes les alertes configurées de type Type d'alerte) pour afficher toutes les alertes du type d'alerte sélectionné dans un nouvel onglet.

Figure 397: Afficher les règles de déclencheur d'alertes

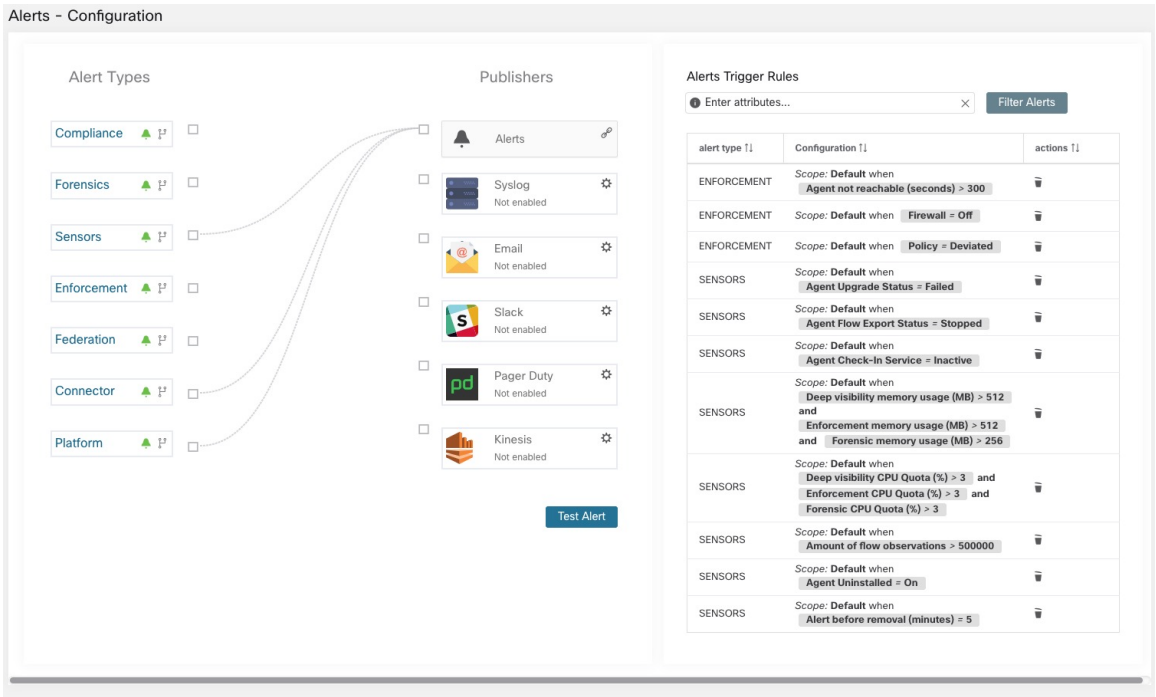
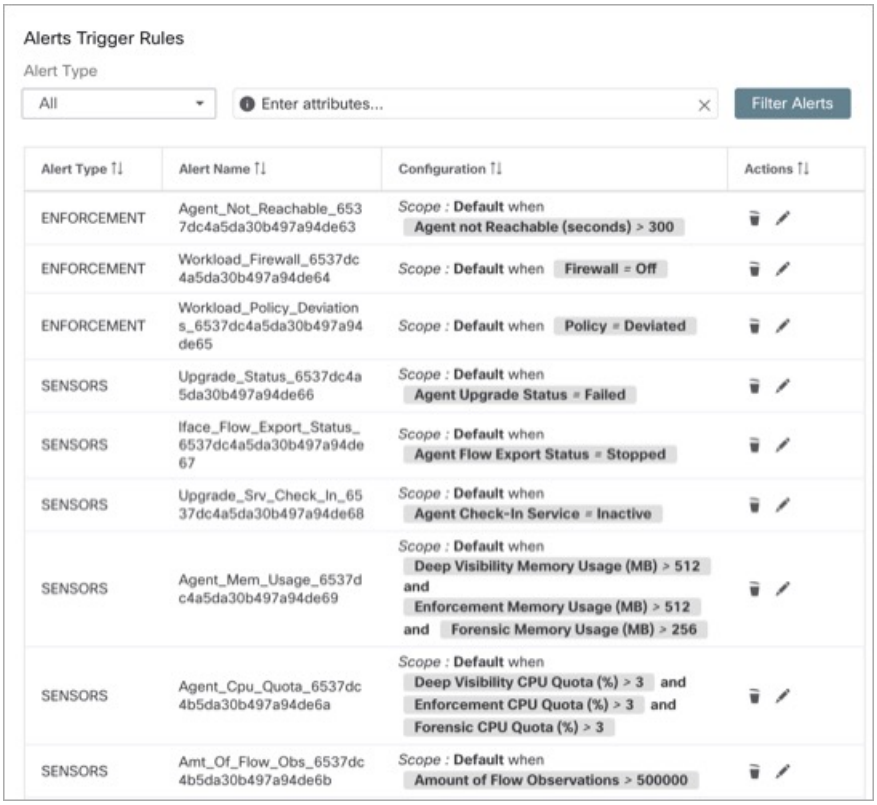


Figure 398: Afficher les règles de déclencheur d'alertes



La fenêtre Règles de déclencheur d'alertes est utilisée pour filtrer les règles de déclencheur d'alertes par type d'alerte et condition de déclencheur.

Note La condition de déclencheur d'alerte est une condition de correspondance exacte.

Détails des règles de déclenchement des alertes

Cliquez sur une ligne de la section **Règles de déclenchement des alertes** pour afficher les détails de la configuration.

1. **Alert Type** : type de l'alerte
2. **Alert Name** : nom de l'alerte.
3. **Configuration** : la condition lorsqu'une alerte est déclenchée dans une portée particulière.

Vous pouvez également afficher d'autres détails comme la **gravité**, les **alertes individuelles** et le **Fréquence des alertes résumées**.

Figure 399: Renseignements détaillés de la configuration des alertes

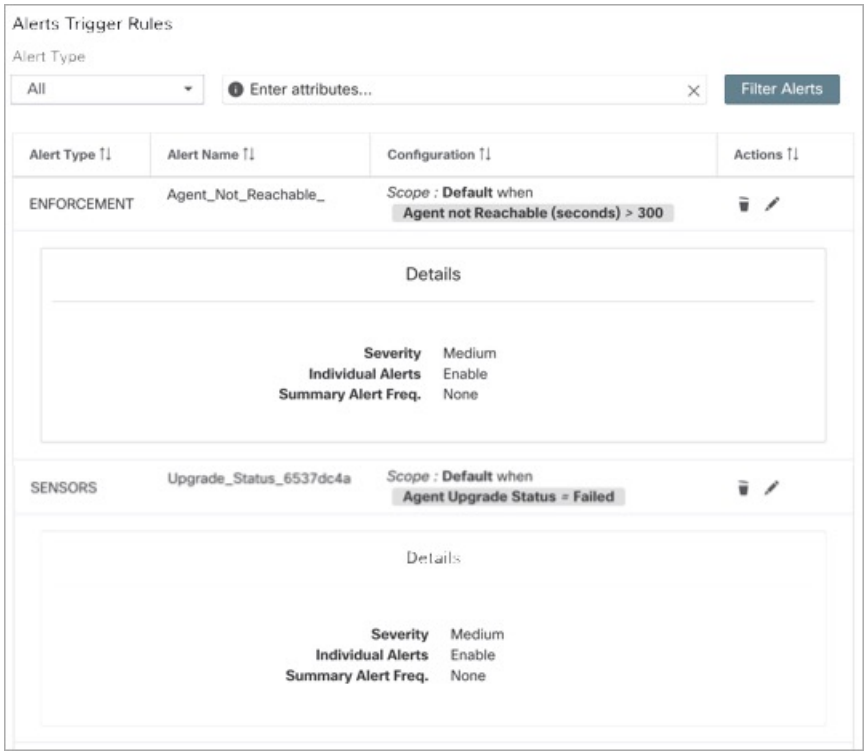
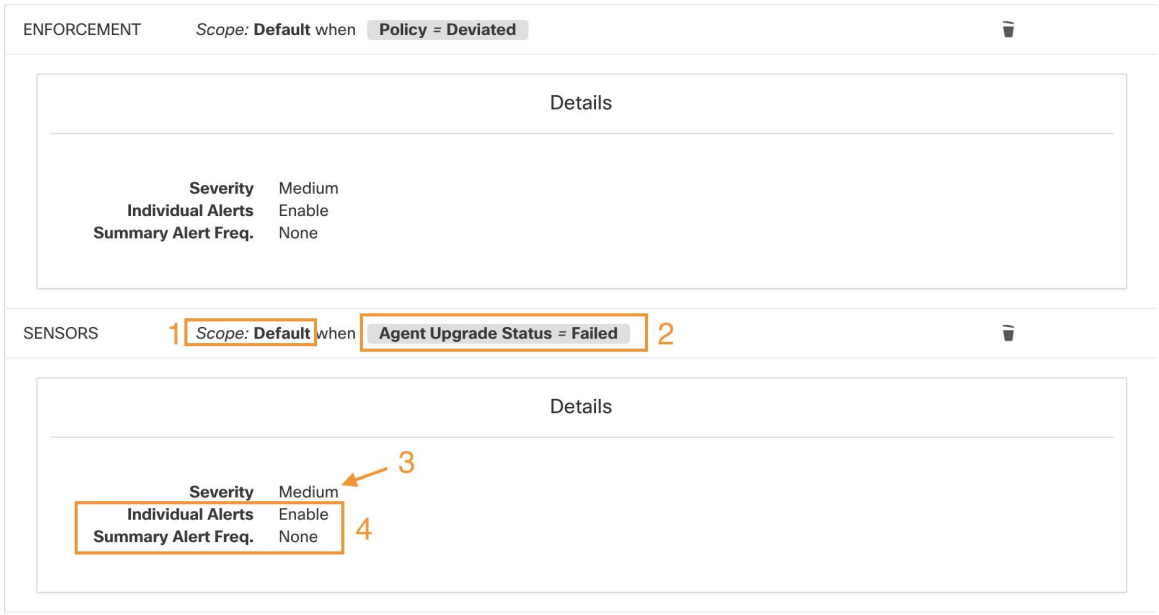


Figure 400: Configuration portée des alertes



Générer des alertes de test

La principale utilisation de la génération d'une alerte de test est de vérifier la connectivité auprès du serveur de publication. Vous pouvez configurer une alerte de test pour envoyer des alertes en fonction du type d'alerte et du serveur de publication lié dans la configuration d'alerte.

Remarque

- La génération d'alertes de test ne se fait pas à partir des sources réelles et est générée à des fins de test uniquement.
- Des alertes de test peuvent être générées pour les types d'alertes liés à au moins un serveur de publication.

Pour générer une alerte de test, procédez comme suit :

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Alerts Config (Configuration des alertes)**.

Étape 2 Pour configurer une alerte de test, cliquez sur **Test Alert** (Tester l'alerte).

Illustration 401 : Configuration des alertes de test

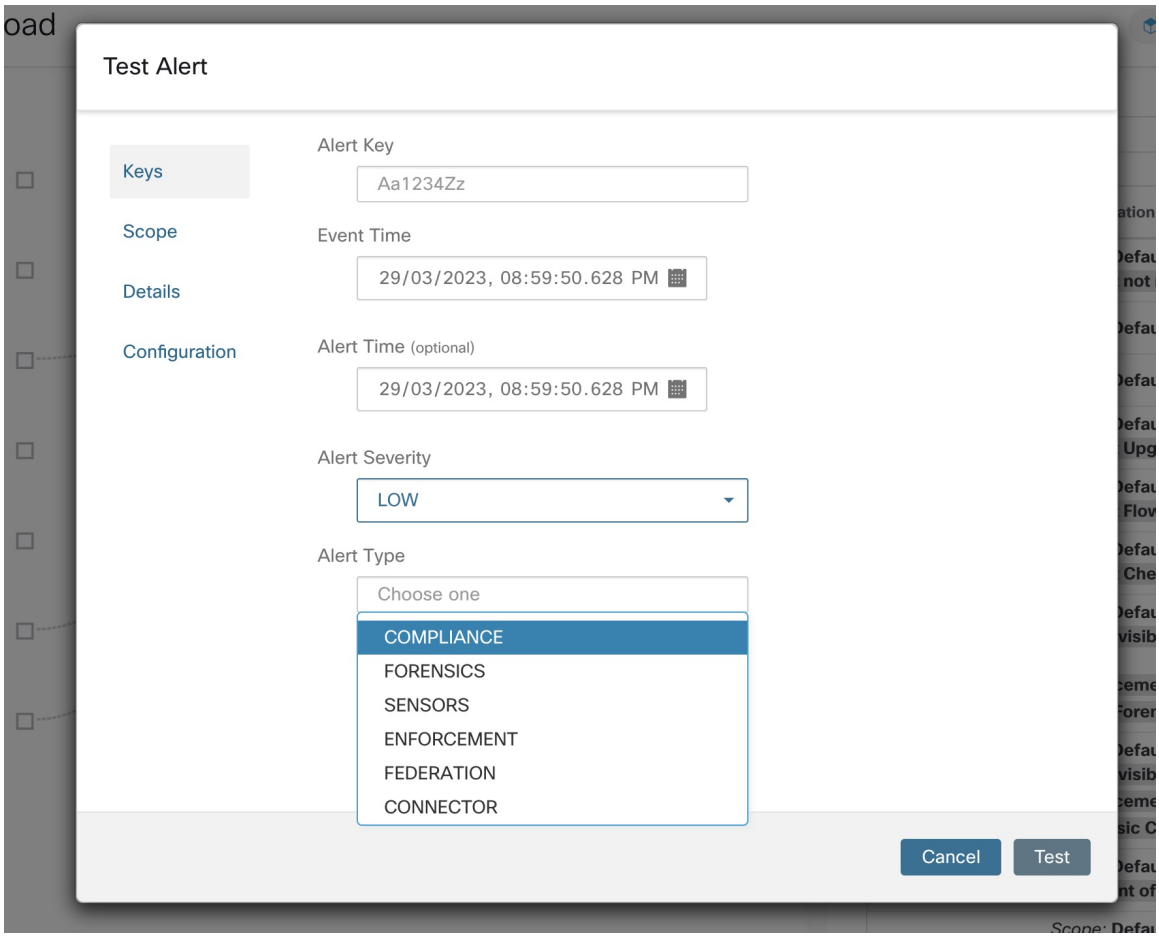
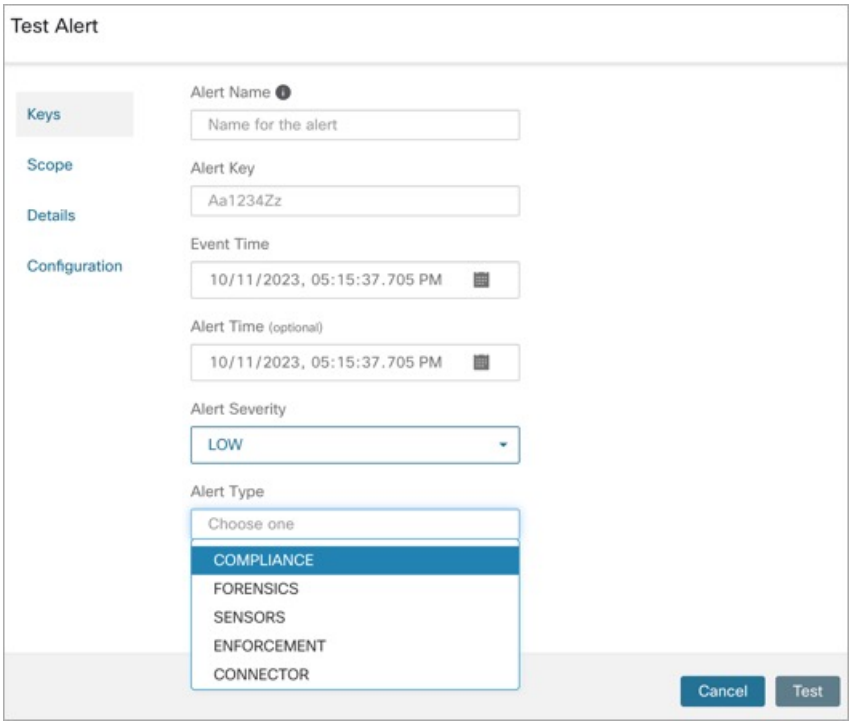


Illustration 402 : Configuration des alertes de test



Étape 3 Sous l'onglet **Keys** (clés), saisissez la valeur pour la clé d'alerte et choisissez les valeurs pour l'heure de l'événement, l'heure de l'alerte, la gravité de l'alerte et le type d'alerte.

Étape 4 Sous l'onglet **Scope** (portée), les valeurs de l'ID de portée et de l'ID du détenteur sont générées automatiquement en fonction de la portée actuelle.

Remarque Si l'ID du détenteur est le même que le VRF de l'ID du détenteur, le système coche automatiquement la case Tenant ID VRF .

Étape 5 Sous l'onglet **Details** (détails), saisissez les valeurs pour le texte de l'alerte, les notes d'événement, les détails de l'alerte et l'ID de configuration de l'alerte.

Remarque Les détails de l'alerte peuvent être une chaîne ou des données au format JSON.

Les options pour le contenu JSON sont les suivantes :

1. Contenant les champs attendus par ce type d'alerte.
2. Tout exemple de données JSON, si ce type d'alerte n'attend pas de champs json par défaut.

   Exemple de JSON :

   ```
   {"alert_name ":"sample","alert_category":{"severity": "dummy"}}
   ```

Étape 6 Sous l'onglet **Configuration** (configuration), choisissez la valeur pour l'alerte individuelle, la fréquence des alertes et le résumé de la fréquence des alertes.

Pour des alertes individuelles, choisissez *ENABLE* (activer) ou *DISABLE* (Désactiver) dans la liste déroulante.

La fréquence des alertes est sélectionnée automatiquement et la fréquence est *INDIVIDUAL* (INDIVIDUELLE).

Remarque Elle prend uniquement en charge les alertes individuelles et ne prend pas en compte la récapitulation.

L'alerte récapitulative est automatiquement sélectionnée à *NONE* (AUCUNE).

Étape 7 Pour générer l'alerte de test, cliquez sur **TEST**.

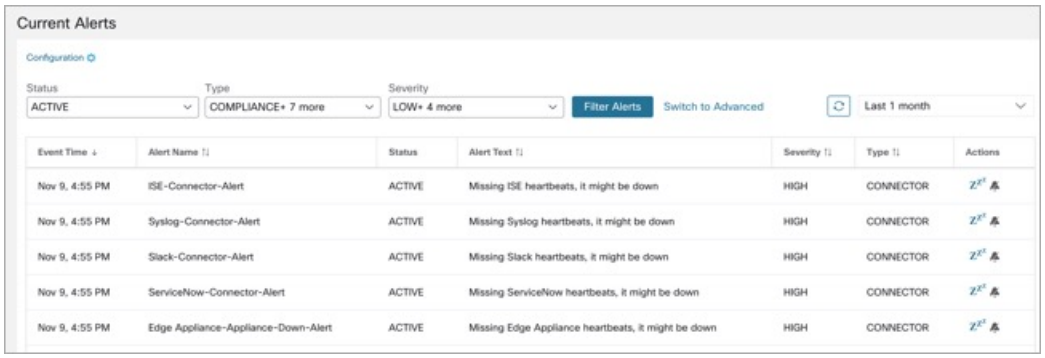
Remarque Une alerte de test est générée et envoyée au serveur de publication configuré.

Alertes actuelles

Accédez à la page **Investigate** (Enquêter) > **Alerts (Alertes)** pour afficher la liste de toutes les alertes actives. Vous pouvez filtrer les alertes par **état**, **type**, **gravité** et plage temporelle.

Seules les alertes dont la gravité est définie sur IMMEDIATE_ACTION, CRITICAL, HIGH, MEDIUM, ou LOW (IMMÉDIAT_ACTION, CRITIQUE, ÉLEVÉE, MOYENNE ou FAIBLE) sont affichées dans la page **Current Alerts** Alertes actuelles). Toutes les alertes, quelles que soient les valeurs de gravité, sont envoyées au broker Kafka configuré.

Figure 403: Alertes actuelles



Filtrer les alertes par plage temporelle

1. Choisissez une valeur dans la liste déroulante. La valeur par défaut est 1 mois.
2. Cliquez sur **Personnalisé** et remplissez les dates **Du** et **Au** pour configurer une plage personnalisée. Cliquez sur **Apply**. Notez que lorsqu'une plage temporelle personnalisée est sélectionnée, le bouton **Refresh** (Actualiser) est désactivé.

Filtrage avancé

1. Cliquez sur **Basculer vers les fonctions avancées**.
2. Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'**information** pour afficher les propriétés à filtrer.

   Les filtres d'alerte ne sont pas conservés lorsque vous revenez aux options de base.

Afficher des détails supplémentaires sur l'alerte

Vous pouvez afficher plus de détails en cliquant sur une alerte.

Figure 404: Détails de l'alerte

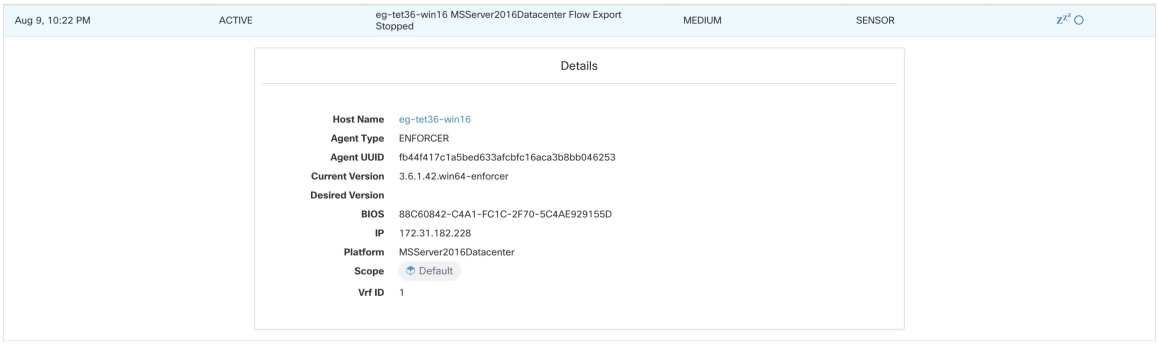
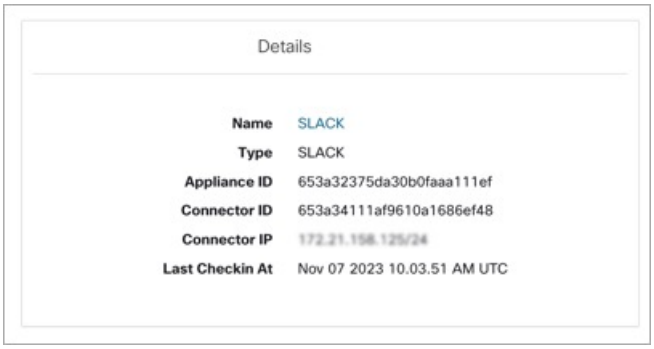


Figure 405: Détails de l'alerte



- Seules 60 alertes par minute et par portée racine sont affichées. Un volume d'alertes plus élevé entraîne un type d'alerte appelé alertes récapitulatives, avec un nombre d'alertes qui ne sont pas affichées .
- Il y a un nombre maximal d'alertes qui s'affichent à tout moment; les alertes plus anciennes sont abandonnées au fur et à mesure que de nouvelles alertes arrivent.

  Pour en savoir plus, consultez la section Limites de configuration dans Cisco Secure Workload.

Répéter les alertes

L'application Alerts (Alertes) permet de répéter des alertes du même type pour une durée donnée. Le type d'alerte est défini différemment selon l'espace de travail pour lequel l'alerte est actuellement configurée. Par exemple, le type d'alerte de conformité est défini selon quatre dimensions : portée du consommateur, portée du fournisseur, protocole et port du fournisseur.

Note Actuellement, vous ne pouvez pas répéter ou désactiver le son des alertes créées par l'application de l'utilisateur.

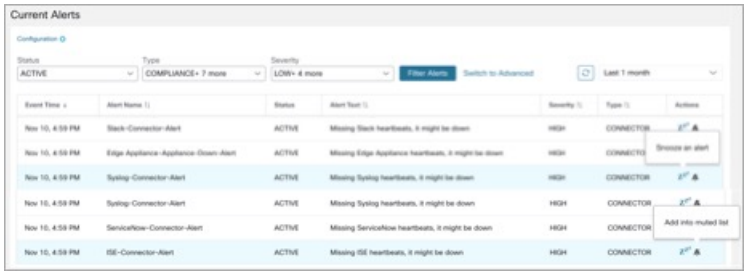
Répéter ou désactiver une alerte

Répéter les alertes :

1. Sous **Actions**, cliquez sur l'icône **Snooze** (Répéter).

2. Choisissez un intervalle dans la liste déroulante.
3. Cliquez sur **Snooze** (Répéter).

Figure 406: Répéter une alerte



Mute Alert (Désactiver l'alerte) :

Utilisez l'option de mise en sourdine pour ne plus recevoir d'alertes.

1. Sous **Actions**, cliquez sur l'icône **Mute** (Désactiver l'alerte, la mettre en sourdine).
2. Pour confirmer, cliquez sur **Yes** (Oui).

   Pour réactiver le son, supprimez l'alerte de la liste des mises en sourdines. Utilisez le menu déroulant de filtre **Status** (État du filtre) pour afficher toutes les alertes **MUTED** (Mises en sourdines) et réactivez le son de l'alerte requise.

Note Vous pouvez afficher jusqu'à 5 000 alertes mises en sourdine ou répétées en attente dans une portée.

Alertes Admiral

Admiral est un système d'alerte intégré, qui remplace le système Bosun des versions précédentes. Pour obtenir plus de renseignements, reportez-vous à la section sur les alertes Admiral.

Détails de l'alerte

Structure commune des alertes

Toutes les alertes respectent une structure globale commune. La structure correspond à la structure de message json disponible par l'intermédiaire de dérivations de données Kafka.

Champ	Format	À propos de
root_scope_id	chaîne	ID de la portée correspondant à la portée supérieure dans la hiérarchie des portées.

Champ	Format	À propos de
key_id	chaîne	id utilisé pour déterminer les alertes « similaires ». Les key_id identiques peuvent être répétés.
type	chaîne	Type de l'alerte. Ensemble fixe de valeurs de chaîne : COMPLIANCE, USERAPP, FORENSICS, ENFORCEMENT, SENSOR, PLATFORM, FEDERATION, CONNECTOR
event_time	long	Horodatage du déclenchement de l'événement (ou si l'événement s'étend sur une plage, le début de la plage). Cet horodatage est en heure d'origine en millisecondes (UTC).
alert_time	long	Horodatage de la première tentative d'envoi de l'alerte. Ce sera après la plage temporelle de l'événement. Cet horodatage est en heure d'origine en millisecondes (UTC).
alert_text	chaîne	Titre de l'alerte.
alert_text_with_names	chaîne	Même contenu que alert_text, mais tous les champs ID sont remplacés par le nom correspondant. Ce champ peut ne pas exister pour toutes les alertes.
gravité	chaîne	Ensemble de valeurs de chaînes fixe : LOW, MEDIUM, HIGH, CRITICAL, IMMEDIATE_ACTION. Il s'agit de la gravité de l'alerte. Pour certains types d'alertes, ces valeurs sont configurables.
alert_notes	chaîne	Généralement non défini. Peut exister dans certains cas particuliers pour la transmission d'informations supplémentaires par Kafka DataTap.
alert_conf_id	chaîne	ID de la configuration d'alerte qui a déclenché cette alerte. Peut ne pas exister pour toutes les alertes.

Champ	Format	À propos de
alert_details	chaîne	Données structurées json sous forme de chaîne de caractères. Consultez les détails de la fonctionnalité pour un type d'alerte spécifique, car la structure exacte de ce champ varie en fonction du type d'alerte.
alert_details_json	json	Même contenu qu'alerte_détails, mais sans chaîne de caractères. Présent uniquement pour les alertes de conformité et uniquement par l'intermédiaire de Kafka.
tenant_id	chaîne	Peut contenir un VRF correspondant à root_scope_id. Ou peut contenir 0 comme valeur par défaut. Il peut aussi ne pas être présent du tout.
alert_id	chaîne	ID temporaire généré en interne. Il est préférable de l'ignorer.
alert_name	chaîne	Nom de l'alerte.

- Conformité : lab- compliance-alert-details
- Criminalistique : Intégration externe et Champs affichés dans les événements criminalistiques
- Capteur : Détails de l'alerte de capteur
- Mise en application : Détails de l'alerte d'application
- Connecteur : détails de l'alerte

Types d'alertes supplémentaires pour les grappes sur site

- Fabric (Structure) : fabric-alerte-details
- Fédération : federation-alert-details
- Plateforme : Détails de l'alerte

- Fédération : federation-alert-details
- Plateforme : Détails de l'alerte

Format général de l'alerte par outil de notification

Voici des exemples de l'affichage des alertes pour différents types de notifications.

Note À partir de la version 3.9 de Cisco Secure Workload, les détails de l'émetteur de la notification comprennent **Alert Name**.

Kafka (Surveillance de données)

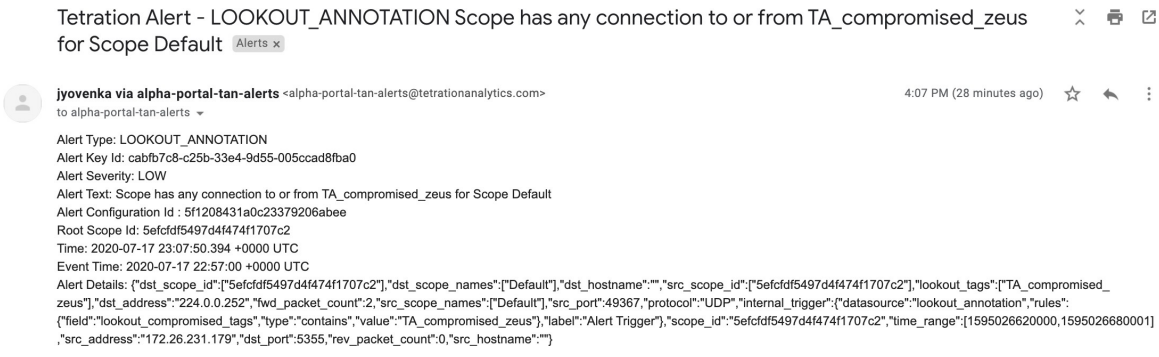
Les messages Kafka (DataTap) sont au format JSON. l'exemple ci-dessous; consultez la section alert_details ci-dessus pour obtenir des exemples supplémentaires.


```
  {
  "severity": "LOW",
  "tenant_id": 0,
  "alert_time": 1595207103337,
  "alert_text": "Lookout Annotated Flows contains TA_zeus for
<scope_id:5efcfdf5497d4f474f1707c2>",
  "key_id": "0a4a4208-f721-398c-b61c-c07af3be9413",
  "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION_PARQUET',
 location_name='lookout_annotation', location_grain='HOURLY',
root_scope_id='5efcfdf5497d4f474f1707c2'}/bd33f37af32a5ce71e888f95ccfe845305e61a12a7829ca5f2d72bf96237d403",

  "alert_text_with_names": "Lookout Annotated Flows contains TA_zeus for Scope Default",
  "root_scope_id": "5efcfdf5497d4f474f1707c2",
  "alert_conf_id": "5f10c7141a0c236b78148da1",
  "type": "LOOKOUT_ANNOTATION",
  "event_time": 1595204760000,
  "alert_details":
"{\"dst_scope_id\":[\"5efcfdf5497d4f474f1707c2\"],\"dst_scope_names\":[\"Default\"],\"dst_hostname\":\"\",\"src_scope_id\":[\"5efcfdf5497d4f474f1707c2\"],\"lookout_tags\":[\"TA_compromised_zeus\"],\"dst_address\":\"224.0.0.252\",\"fwd_packet_count\":2,\"src_scope_names\":[\"Default\"],\"src_port\":49367,\"protocol\":\"UDP\",\"internal_trigger\":{\"datasource\":\"lookout_annotation\",\"rules\":[{\"field\":\"lookout_compromised_tags\",\"type\":\"contains\",\"value\":\"TA_compromised_zeus\"}],\"label\":\"Alert Trigger\"},\"scope_id\":\"5efcfdf5497d4f474f1707c2\",\"time_range\":[1595026620000,1595026680001],\"src_address\":\"172.26.231.179\",\"dst_port\":5355,\"rev_packet_count\":0,\"src_hostname\":\"\"}"

  }
```


Courriel

Renseignements sur la configuration des alertes par courriel : Connecteur de courriel

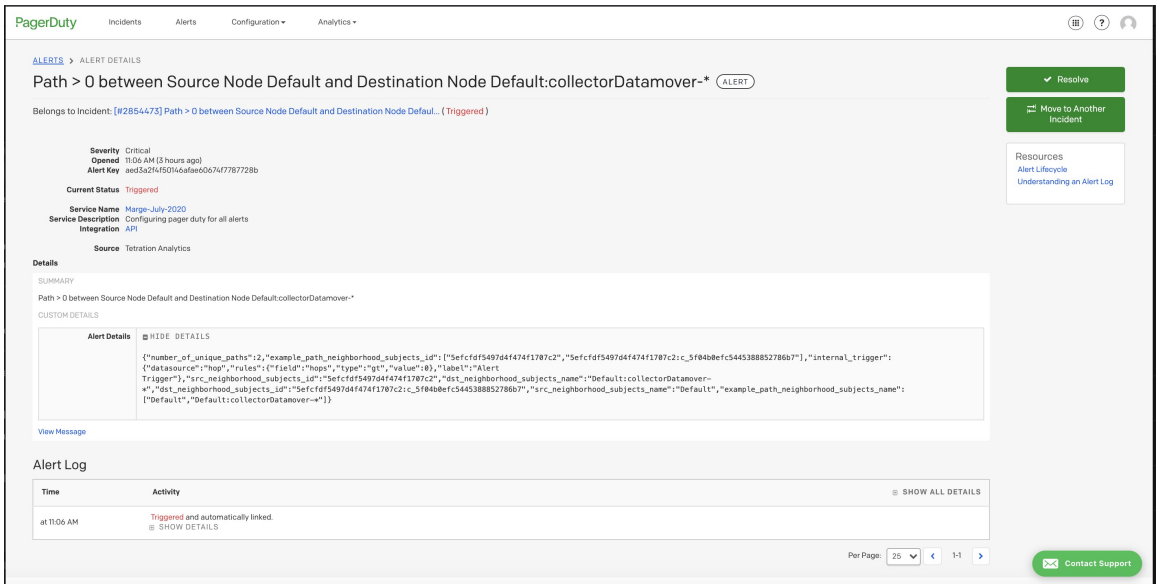
Figure 407: Exemple d'alerte Cisco Cisco Secure Workload



PagerDuty

Renseignements sur la configuration des alertes de PagerDuty : Connecteur PagerDuty

Figure 408: Exemple d'alerte Cisco Secure Workload dans PagerDuty



Les alertes envoyées à PagerDuty sont un nouveau déclenchement de la même alerte en fonction de key_id.

La gravité est mappée à la gravité PagerDuty comme suit :

Gravité Cisco Secure Workload	Gravité PagerDuty
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	critique
CRITIQUE	critique
ÉLEVÉE	erreur
MOYENNE	avertissement
FAIBLE	Information

Syslog

Informations sur la configuration des alertes Syslog et le réglage du mappage de gravité : Connecteur Syslog

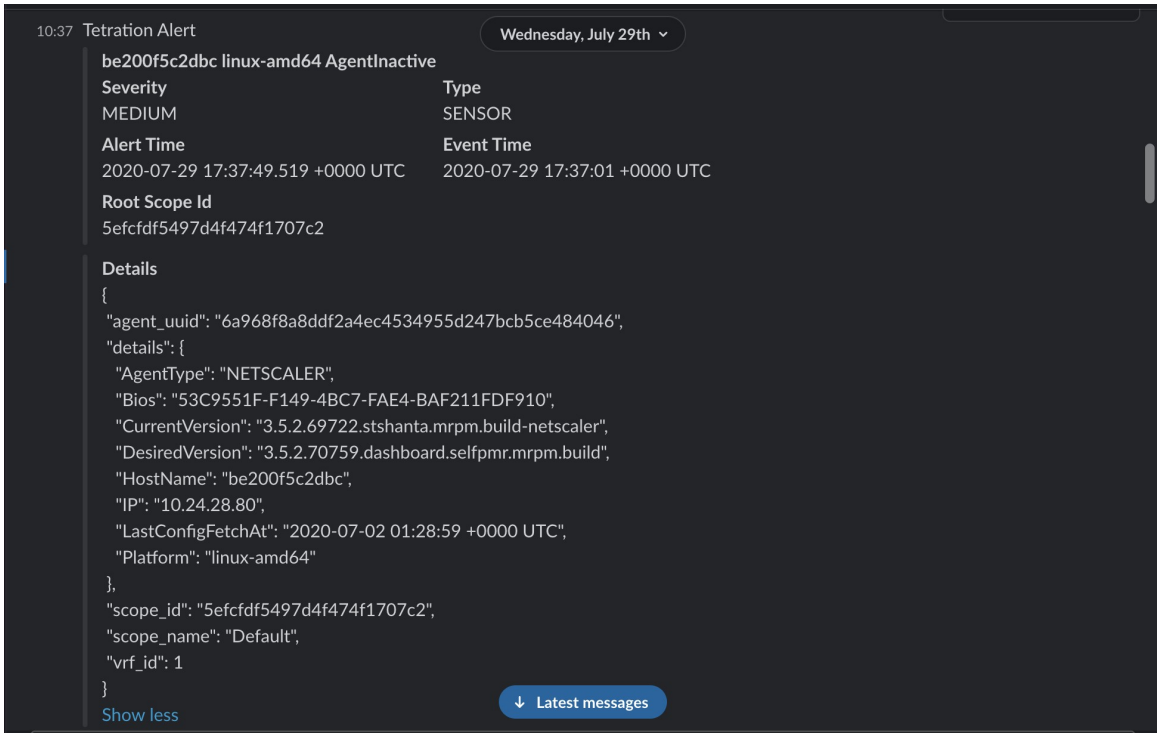
Figure 409: Exemple de plusieurs alertes Cisco Secure Workload envoyées à syslog

Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"3ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":53,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":37367,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.139\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":39652,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.137\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":63811,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.136\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":57418,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.138\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53},{\"consumer_port\":12599,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.141\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53},{\"consumer_port\":7385,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.140\",\"provider_address\":\"173.36.131.10\",\"provider_port\":53}],\"escaped_count\":6,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"UDP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"8f0cfcb5-f8c1-3130-a069-3721b7d50159","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":5660,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17131,\"protocol\":\"TCP\",\"consumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.140\",\"provider_port\":5660}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope_names\":[\"Default\"],\"provider_port\":443,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17792,\"protocol\":\"TCP\",\"consumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.133\",\"provider_port\":443}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}

Slack

Informations sur la configuration des alertes Slack : Connecteur Slack

Figure 410: Exemple d'alerte Cisco Secure Workload envoyée au canal Slack



Kinesis

Renseignements sur la configuration des alertes Kinesis : Connecteur Kinesis

Les alertes Kinesis sont similaires aux alertes Kafka, car ce sont deux files d'attente de messages.

CHAPITRE 11

Entretien de la grappe

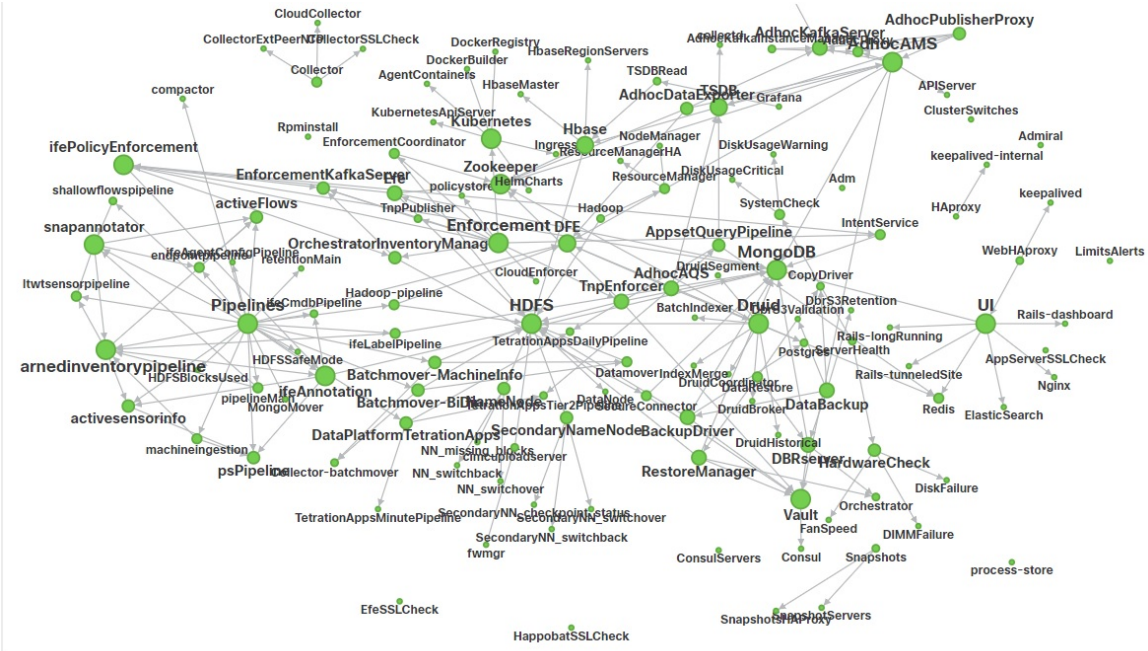
Ce chapitre fournit des détails sur les diverses actions de maintenance de la grappe que vous pouvez effectuer, telles que la mise à niveau, le redémarrage, la planification de sauvegardes de données et la restauration de données. Vous pouvez également afficher l'état du service et de la grappe à partir des options disponibles dans le menu de **dépannage**.

État du service

Dans le volet de navigation de gauche, la page **Troubleshoot (Dépannage)** > **Service Status (État du service)** affiche l'intégrité de tous les services utilisés dans votre grappe Cisco Cisco Secure Workload ainsi que leurs dépendances.

La vue graphique affiche l'intégrité du service, chaque nœud du graphique affiche l'intégrité du service et une périphérie représente la dépendance à l'égard d'autres services. Les services non intègres sont signalés en rouge lorsque le service n'est pas disponible et en orangé lorsque le service est défaillant mais disponible. Un nœud vert indique que le service est intègre. Pour plus d'informations de débogage sur ces nœuds, utilisez l'arborescence qui comporte le bouton **Expand All** (Tout développer) pour afficher tous les nœuds enfants dans l'arborescence des dépendances. « En panne » indique que le service n'est pas fonctionnel et « Non intègre » indique que le service n'est pas entièrement fonctionnel.

Figure 411: Page État du service



Alertes Admiral

Admiral est un système d'alerte intégré. Il traite les alertes en fonction de l'intégrité du service signalée par le État du service (État du service). Ainsi, les utilisateurs disposent d'un moyen unifié de déterminer l'intégrité d'un service ou de la grappe. L'état du service affiche l'intégrité actuelle (à un moment donné) d'un service. Le service est considéré comme en panne lorsqu'il indique l'état du service en rouge, sinon il est considéré comme activé. La disponibilité est le moment où le service est signalé comme opérationnel. Admiral évalue l'intégrité du service signalée par état de service au fil du temps et déclenche une alerte si le pourcentage de disponibilité du service tombe sous un certain seuil. Cette évaluation sur une certaine durée garantit que nous réduisons les faux positifs et que nous alertons uniquement en cas de pannes de service réelles.

Comme les services ont des besoins en alertes différents, ce pourcentage et cet intervalle de temps sont fixés différemment pour chaque service.

Les clients peuvent utiliser les notifications Admiral pour être informés de ces événements. Elles sont également visibles sur la page **Investigate (Enquêter)** > **Alerts (Alertes)** , sous le type PLATFORM (PLATEFORME).

Note Seul un sous-ensemble de services choisi est associé à une alerte Admiral. Si un service ne fait pas partie du sous-ensemble ci-dessus, aucune alerte Admiral ne sera déclenchée lors de sa panne. Ce sous-ensemble de services avec alertes Admiral, leurs pourcentages de seuil d'alerte et leurs intervalles de temps est fixe et n'est pas configurable par l'utilisateur.

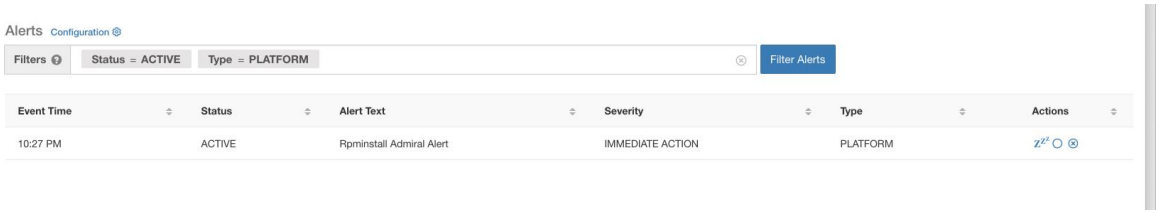
Les sections suivantes décrivent plus en détail les alertes et les notifications Admiral.

Cycle de vie d'une alerte Admiral

L'Admiral vérifie la disponibilité des services sur l'état des services. Il déclenche une alerte lorsque ce temps de disponibilité devient inférieur au seuil d'alerte préconfiguré.

Par exemple, Rpminstall est un service utilisé pour installer les RPM lors des déploiements, des mises à niveau, des correctifs, etc. Il est configuré pour générer une alerte Admiral si son temps de disponibilité est inférieur à 80 % sur une heure. Si le service Rpminstall tombe en panne pendant une durée supérieure au seuil précisé ci-dessus, une alerte Admiral est générée pour Rpminstall avec l'état ACTIVE.

Figure 412: Alerte Admiral active



Lorsque le service se rétablit, son pourcentage de disponibilité commence à augmenter. Lorsque la disponibilité dépasse son seuil, l'alerte se ferme automatiquement et son état passe à CLOSED (FERMÉE). Dans l'exemple Rpminstall décrit ci-dessus, RpminstallAdmiral Alert se ferme automatiquement lorsque son temps de disponibilité dépasse 80 % en une heure.

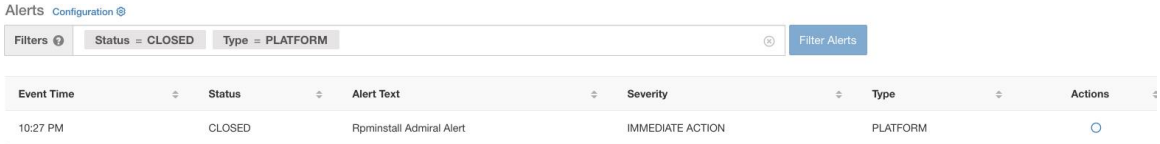
Note La fin de l'alerte est TOUJOURS décalée par rapport au retour à la normale du service. En effet, Admiral examine l'intégrité du service sur une période donnée. Dans l'exemple ci-dessus, puisque le seuil d'alerte Rpminstall est défini à 80 % d'une heure de disponibilité, il doit l'être depuis au moins 48 minutes (80 % d'une heure) avant que l'alerte ne se ferme.

Aucune action n'est requise pour fermer l'alerte. Ainsi, toutes les alertes Admiral ACTIVENT indiquent un problème sous-jacent nécessitant notre attention.

Note Aucune notification dédiée n'est générée à la fermeture des alertes.

Après qu'une alerte soit passée à FERMÉE, elle ne s'affichera plus sous les alertes ACTIVES. Les alertes fermées peuvent toujours être vues sur l'interface utilisateur en utilisant le filtre Status=CLOSED comme indiqué ci-dessous :

Figure 413: Fermeture automatique d'alerte Admiral à la reprise du service



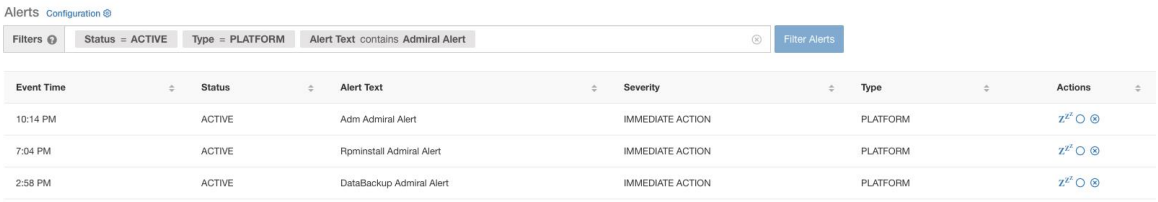
Il existe deux types d'alertes Admiral :

- Alerte Admiral individuelle
- Résumé des alertes Admiral

Alerte Admiral individuelle

Les alertes décrites dans la section précédente, les alertes qui sont déclenchées pour des services individuels, appartiennent à la catégorie d'alerte individuelle Admiral. Le texte de l'alerte contient toujours l <*Service Name*> de l'alerte Admiral. Cela facilite le filtrage des alertes individuelles par service ou par le suffixe **Admiral Alert**.

Figure 414: Filtre de texte d'alerte pour les alertes Admiral individuelles

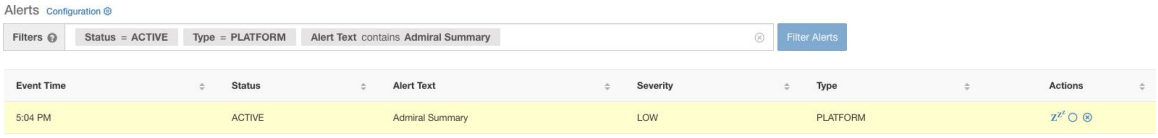


Résumé des alertes Admiral

Admiral génère des alertes résumées quotidiennement à minuit UTC. Elles contiennent une liste des alertes actuellement actives et de toutes les alertes fermées au cours de la dernière journée. Cela permet à l'utilisateur de voir l'intégrité globale de la grappe signalée par Admiral en un seul endroit. C'est également utile pour constater les alertes fermées qui ne génèrent pas de notification dédiée autrement. Si la grappe est intègre et qu'aucune alerte n'a été fermée au cours de la dernière journée, aucune notification récapitulative n'est générée pour ce jour-là. Cela sert à réduire les notifications et le bruit informationnel inutiles.

Le texte des alertes, dans ce cas, est toujours **« Admiral Summary** » . Cela facilite le filtrage des alertes résumées, comme le montre la figure suivante.

Figure 415: Filtre de texte de résumé Admiral



Détails de l'alerte

Alertes individuelles

Lorsque l'on clique sur l'alerte pour une alerte de type Admiral, celle-ci se déploie pour afficher des champs utiles au débogage et à l'analyse de l'alerte.

Figure 416: Détails de l'alerte

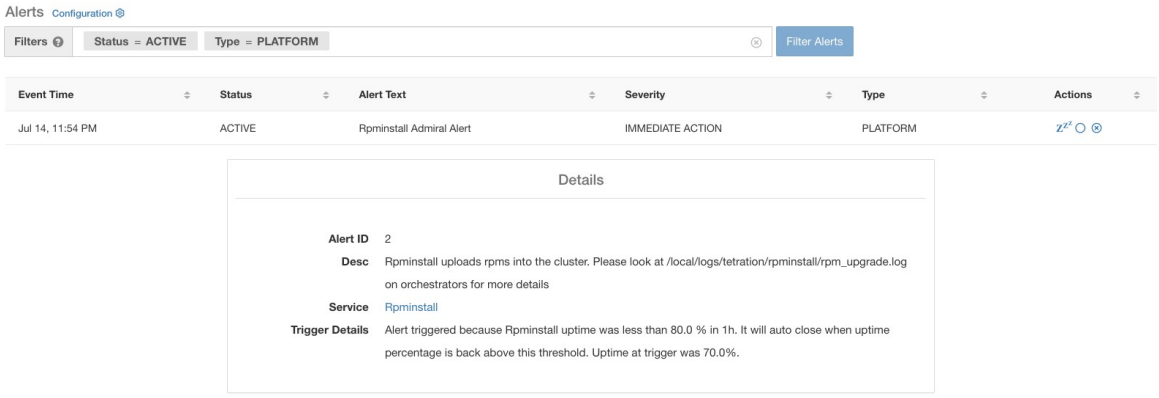


Table 34: Description des champs des détails de l'alerte

Champ	Description
ID d'alerte	Identifiant unique pour les alertes. Cela permet d'identifier un cas particulier de défaillance d'un service. Comme indiqué précédemment, lorsque le temps de fonctionnement sous-jacent du service signalé par l'alerte devient normal, l'alerte se ferme automatiquement. Si le même service tombe en panne ensuite, une nouvelle alerte avec un ID d'alerte différent est générée. L'identifiant de l'alerte permet donc d'identifier chaque cas de déclenchement de l'alerte.
Desc	Le champ de description contient des renseignements supplémentaires sur le problème de service à l'origine de l'alerte.
Service	Celui-ci contient un lien conduisant l'utilisateur à la page d'état du service où ce dernier peut être consulté. L'utilisateur peut également obtenir plus de détails sur les raisons pour lesquelles le service est signalé dans la page d'état du service.
Détails du déclencheur	Ceci contient les détails sur les seuils de déclenchement pour le service. Ces seuils permettent à l'utilisateur de savoir à quel moment l'alerte doit être clôturée après le rétablissement du service sous-jacent. Par exemple, le seuil RPMinstall est indiqué comme suit : 80 % de disponibilité sur une heure. Par conséquent, le service RPMinstall doit être actif depuis au moins 48 minutes (80 % d'une heure) avant que l'alerte ne se ferme automatiquement. Cela affiche également la valeur de disponibilité observée pour le service lorsque l'alerte a été déclenchée.

Voici un exemple de sortie de Kafka JSON :

```
  {
  "severity": "IMMEDIATE_ACTION",
  "tenant_id": 0,
  "alert_time": 1595630519423,
  "alert_text": "Rpminstall Admiral Alert",
  "key_id": "ADMIRAL_ALERT_5",
  "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/66eb975f5f987fe9eaefa81cee757c8b6dac5facc26554182d8112a98b35c4ab",

  "root_scope_id": "5efcfdf5497d4f474f1707c2",
  "type": "PLATFORM",
  "event_time": 1595630511858,
  "Check  /local/logs/tetration/rpminstall/rpm_upgrade.log on
orchestrators for more details\",\"Trigger Details\":\"Alert triggered because Rpminstall
uptime was less than 80.0 % in 1h. It will auto close when uptime percentage is back above
this threshold. Uptime at trigger was 65.0%. \"}"
  }
```

Toutes les alertes individuelles respectent le format JSON Kafka. Les services (à partir de l'état du service) qui sont couverts par la surveillance Admiral sont énumérés dans le tableau suivant :

Table 35: Services couverts par la surveillance Admiral

Service	Conditions de déclenchement	Gravité
Serveur API Kubernetes	La disponibilité du service est inférieure à 90 % au cours des 15 dernières minutes	ACTION IMMÉDIATE
Administrateur	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE
Sauvegarde des données	La disponibilité du service est inférieure à 90 % au cours des 6 dernières heures.	ACTION IMMÉDIATE
Utilisation disque critique	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Redémarrage requis	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE
RPMinstall	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
SecondaryNN_checkpoint_status	La disponibilité du service est inférieure à 90 % au cours de la dernière heure.	ACTION IMMÉDIATE

Pour les grappes physiques de 8 ou 39 RU, les services suivants sont également surveillés :

Table 36: Services couverts par la surveillance Admiral pour les grappes de 8 ou 39 RU

Service	Conditions de déclenchement	Gravité
Échec DIMM	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Échec de disque	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Vitesse du ventilateur	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE
Commutateurs en grappe	La disponibilité du service est inférieure à 80 % au cours de la dernière heure.	ACTION IMMÉDIATE

Note La surveillance Admiral s'appuie sur les mesures de traitement générées par l'état du service pour générer des alertes. Si la récupération de la mesure n'est pas possible pendant une durée prolongée (par exemple, si l'état du service est en panne), une alerte (TSDBOracleConnectivity) est déclenchée pour indiquer que le traitement des alertes en fonction du service est désactivé sur la grappe.

Alertes résumées

Les alertes résumées sont de nature informationnelle et sont toujours définies comme de priorité FAIBLE. Lorsque l'on clique sur un résumé d'alerte Admiral, celui-ci se développe pour afficher divers champs contenant des informations résumées sur les alertes Admiral.

Figure 417: Détails de l'alerte résumée Admiral

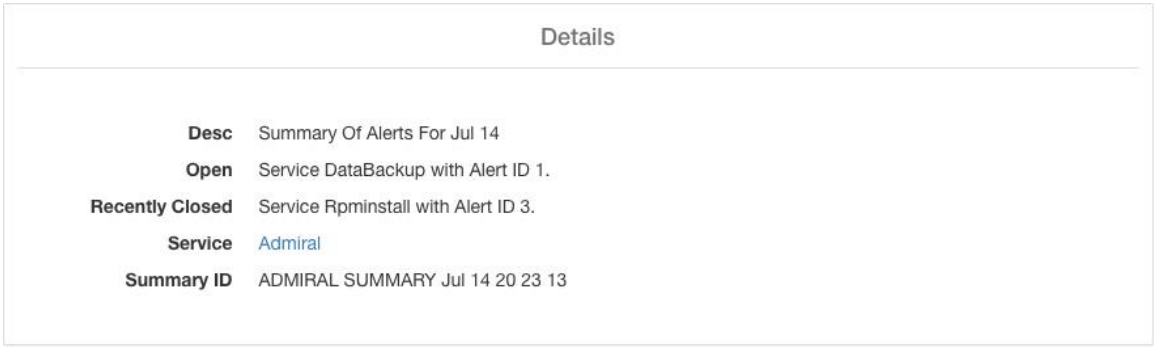


Table 37: Description des champs de l'alerte résumée Admiral

Champ	Description
Desc	Le champ de description contient le jour du résumé quotidien.

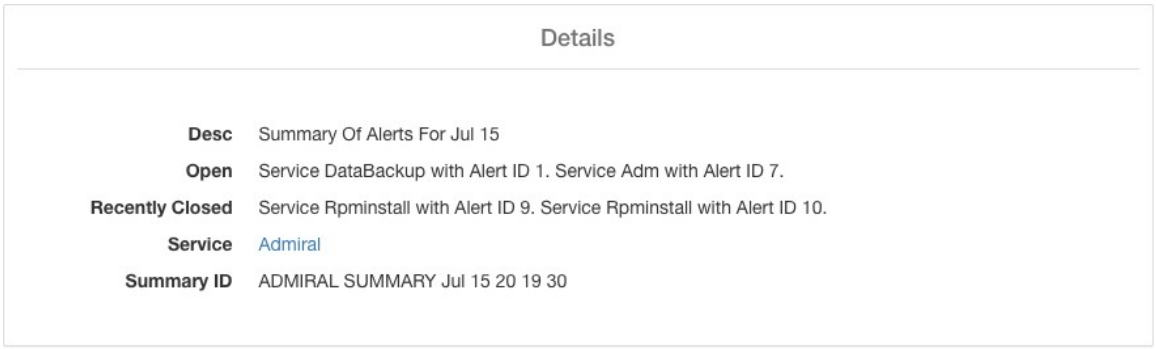
Champ	Description
Ouvert	Les alertes ouvertes indiquent quelles alertes étaient actives lorsque le résumé a été généré.
Fermées récemment	Ceci contient les alertes fermées au cours des dernières 24 heures, c'est-à-dire au cours de la journée pour laquelle le résumé a été généré. L'ID de chaque alerte est également inclus. Étant donné que les alertes se ferment automatiquement, un service donné a pu tomber en panne et créer une alerte, puis revenir à la normale et l'alerte se fermer automatiquement. Il aurait pu le faire plusieurs fois par jour, auquel cas la liste des incidents récemment clôturés comprendra chaque incident ainsi que son numéro d'alerte unique. Toutefois, cela ne devrait pas se produire souvent étant donné que chaque service doit être opérationnel pendant un certain temps avant que l'alerte ne soit clôturée. L'utilisateur peut filtrer avec Status = CLOSED pour obtenir plus d'informations sur chaque incident.
Service	Lien vers l'état du service pour Admiral, qui est le service qui traite et génère le résumé quotidien.
ID du résumé	ID de l'alerte résumée.

Voici un exemple de sortie de Kafka JSON :

```
  {
    "severity": "LOW",
    "tenant_id": 0,
    "alert_time": 1595721914808,
    "alert_text": "Admiral Summary",
    "key_id": "ADMIRAL_SUMMARY_Jul-26-20-00-04",
    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='platform', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/e95da4521012a4789048f72a791fb58ab233bbff63e6cbc421525d4272d469aa",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "PLATFORM",
    "event_time": 1595721856303,
    "alert_details": "{\"Desc\":\"Summary of alerts for Jul-26\",\"Recently
Closed\":\"None\",\"Open\":\" Service Rpminstall with Alert ID
5.\",\"Service\":\"Admiral\",\"Summary ID\":\"ADMIRAL_SUMMARY_Jul-26-20-00-04\"}"
  }
```

Un exemple d'alerte résumée dans laquelle un service déclenche plusieurs alertes dans une journée est présenté ci-dessous :

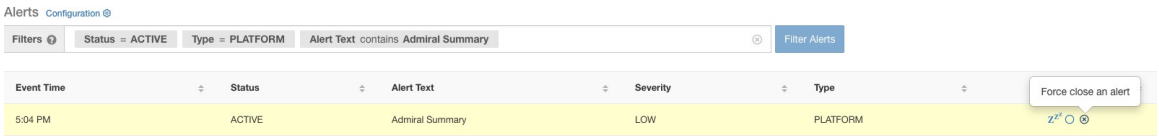
Figure 418: Alertes multiples



Actions des utilisateurs

Puisque les alertes Admiral ne génèrent qu'une seule notification par alerte, l'inclusion, l'exclusion ou la répétition d'alertes précises ne sont pas nécessaires. Les alertes se ferment automatiquement lorsque le service redevient normal pour le seuil de disponibilité, comme décrit ci-dessus. Il existe la possibilité de forcer la fermeture d'une alerte. Normalement, cela ne doit être utilisé que pour supprimer les récapitulatifs des alertes de l'interface utilisateur, car les alertes individuelles se ferment automatiquement.

Figure 419: Forcer la fermeture des alertes

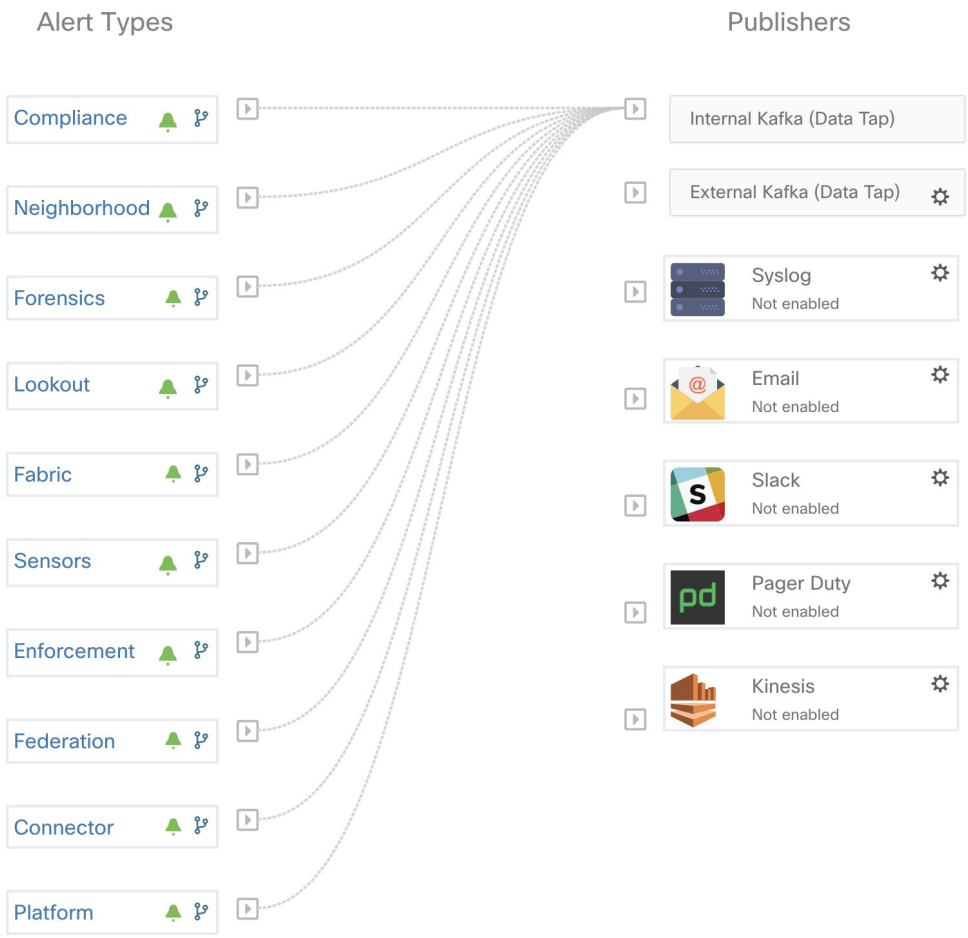


Warning Les alertes individuelles ne doivent pas être fermées de force. Si vous le faites alors que le service sous-jacent est toujours en panne ou que son temps de fonctionnement est inférieur au seuil prévu, une autre alerte sera déclenchée pour le même service lors de la prochaine itération du traitement Admiral.

Notifications Admiral

Les alertes Admiral sont de type PLATFORM. De ce fait, ces alertes peuvent être configurées pour être envoyées à divers annonceurs par les connexions appropriées pour les alertes de plateforme à l'aide de la page de configuration ./configuration. Pour plus de commodité, la connexion est activée entre les alertes de la plateforme et le Kafka interne par défaut, ce qui permet d'afficher les alertes Admiral sur la page Alertes actuelles (aller à **Investigate (Investiguer)** > **Alerts (Alertes)**) sans aucune configuration manuelle.

Figure 420: Configuration des alertes de la plateforme



Les alertes Admiral sont également envoyées à l'adresse courriel configurée sous **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)** > **Admiral Alert Email (Courriel de l'alerte Admiral)**.

Figure 421: Exemple de courriel Admiral

There is a new admiral platform alert on your tetration cluster.
Service: Rpminstall
Start Time: 2020-07-14 23:09 UTC
Alert ID: 3
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

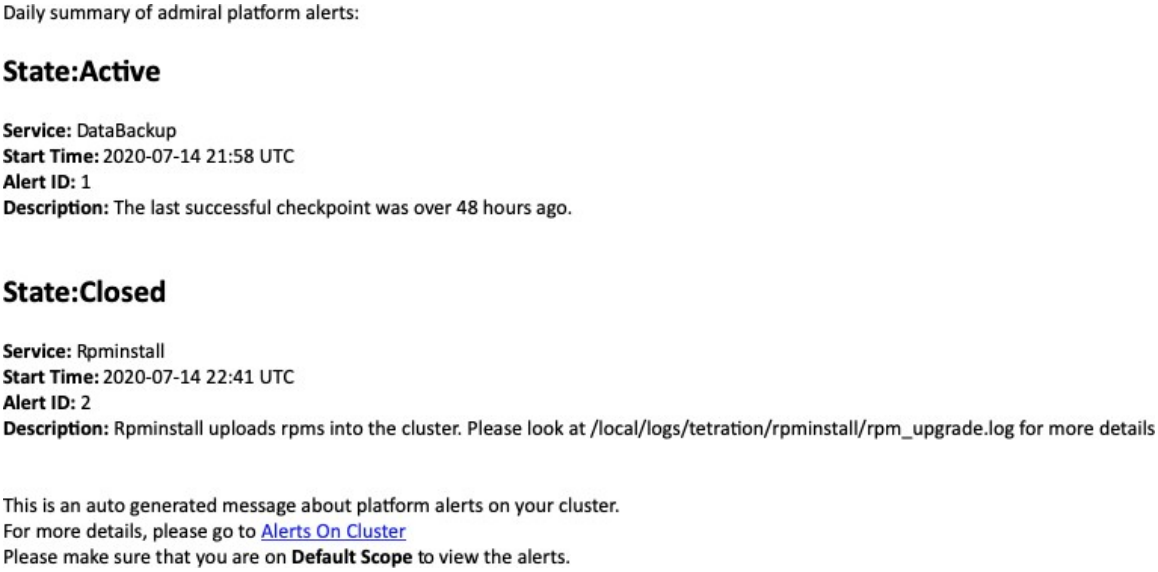
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

Ainsi, les utilisateurs peuvent recevoir des notifications Admiral même s'ils n'ont pas configuré l'appareil TAN Edge. Ce comportement est similaire au comportement du Bosun (maître d'exploitation) dans les versions précédentes.

Figure 422: Adresse courriel de Admiral

Ces notifications par courriel sont générées sur les mêmes déclencheurs que la page Current Alerts (Alertes actuelles). Ainsi, elles sont envoyées lors de la création de l'alerte et lors d'un courriel récapitulatif quotidien à minuit UTC. Le courriel récapitulatif quotidien répertorie toutes les alertes actives et celles fermées au cours des dernières 24 heures.

Figure 423: Exemple de courriel récapitulatif Admiral



Daily summary of admiral platform alerts:

State:Active

Service: DataBackup
Start Time: 2020-07-14 21:58 UTC
Alert ID: 1
Description: The last successful checkpoint was over 48 hours ago.

State:Closed

Service: Rpminstall
Start Time: 2020-07-14 22:41 UTC
Alert ID: 2
Description: Rpminstall uploads rpms into the cluster. Please look at /local/logs/tetration/rpminstall/rpm_upgrade.log for more details

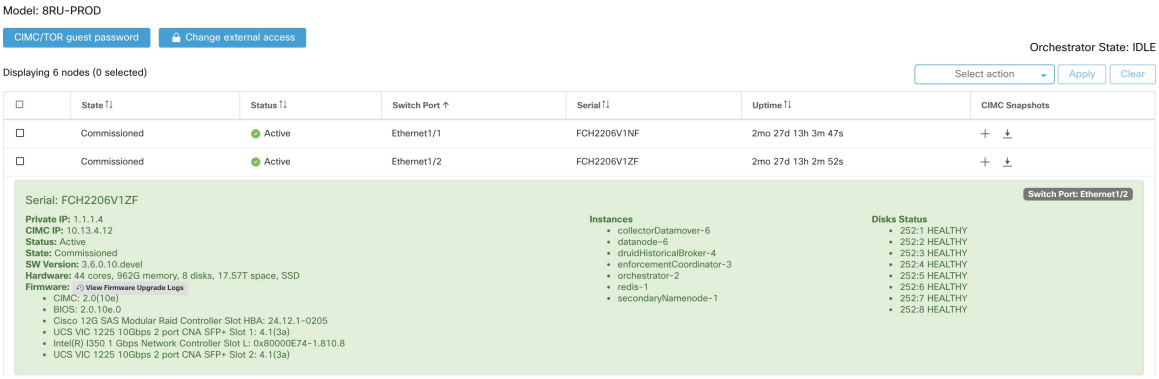
This is an auto generated message about platform alerts on your cluster.
For more details, please go to Alerts On Cluster
Please make sure that you are on **Default Scope** to view the alerts.

S'il n'y a aucune alerte active, ni aucune alerte fermée au cours des dernières 24 heures, les courriels récapitulatifs sont ignorés pour réduire le bruit des courriels.

État de la grappe

La page d' **état de la grappe**, sous le menu **dépannage** dans la barre de navigation de gauche, est accessible aux **administrateurs du site**, mais les actions ne peuvent être effectuées que par les utilisateurs du **service d'assistance à la clientèle**. Il affiche l'état de tous les serveurs physiques du support Cisco Cisco Secure Workload. Chaque ligne du tableau représente un nœud physique avec des détails tels que la configuration de son matériel et de son micrologiciel et l'adresse IP de son contrôleur CIMC (si attribuée). Vous pouvez afficher la vue détaillée du nœud en cliquant sur la ligne . Dans cette page, nous pouvons également modifier le mot de passe CIMC des nœuds et activer ou désactiver l'accès externe. L'état de l'orchestrateur est également affiché sur la page d'état de la grappe pour fournir un contexte au service d'assistance à la clientèle.

Figure 424: État de la grappe



Actions qui affectent tous les nœuds

La modification du mot de passe du contrôleur CIMC et l'activation ou la désactivation de l'accès du contrôleur CIMC externe peuvent être effectuées à l'aide des options **CIMC/TOR guest password** (Mot de passe invité CIMC/TOR) et **Change external access** (modifier l'accès externe). Les actions affectent tous les nœuds de la grappe.

Détails du nœud d'accès du contrôleur CIMC externe

Cliquez sur **Modifier l'accès externe** pour ouvrir une boîte de dialogue qui fournit l'état de l'accès du contrôleur CIMC externe et permet d'activer, de renouveler ou de désactiver l'accès externe à CIMC.

Cliquez sur **Enable** (activer) pour configurer la grappe en arrière-plan pour activer l'accès CIMC externe. Cela peut prendre jusqu'à 60 secondes pour que les tâches soient terminées et que l'accès CIMC externe soit entièrement activé. Lorsque l'accès CIMC externe est activé, une boîte de dialogue s'affiche lorsque l'accès est défini pour expirer automatiquement et **Enable** (activer) passe à **Renew** (Renouveler) pour indiquer que vous pouvez renouveler l'accès CIMC externe. Le renouvellement de l'accès au contrôleur CIMC externe augmente l'heure d'expiration de deux heures par rapport à l'heure actuelle.

Si l'accès CIMC externe est activé, l'adresse IP du contrôleur CIMC dans les détails du nœud (visible en cliquant sur la ligne d'un nœud) devient un lien sur lequel vous pouvez accéder directement à l'interface utilisateur du contrôleur CIMC. Vous devrez peut-être recharger la page d'état de la grappe pour afficher les liens.

Figure 425: Détails du nœud d'accès du contrôleur CIMC externe

L'interface utilisateur du contrôleur CIMC comporte généralement un certificat autosigné. L'accès à l'interface utilisateur du contrôleur CIMC entraînera probablement une erreur dans le navigateur indiquant que le certificat n'est pas valide. Si vous utilisez Google Chrome, vous devrez peut-être taper **`thisisunsafe`** sans guillemets lorsque l'erreur de certificat non valide s'affiche pour contourner la vérification de certificat et accéder à l'interface utilisateur du contrôleur CIMC.

Dans l'interface utilisateur du contrôleur CIMC, l'accès KVM n'est fonctionnel que si la version du contrôleur CIMC est 4.1(1g) ou ultérieure. Une fois l'accès CIMC externe activé, il est automatiquement désactivé au bout de deux heures, sauf si l'accès est renouvelé ou désactivé.

La désactivation de l'accès CIMC externe configure la grappe en arrière-plan pour désactiver l'accès CIMC externe. Cela peut prendre jusqu'à 60 secondes pour que la tâche se termine et que l'accès CIMC externe soit complètement désactivé.

Table 38: Détails du nœud physique

Champ	Description
État	Le champ **Status** (État) indique l'état de l'alimentation du nœud. Les valeurs possibles sont les suivantes : • **Actif** : le nœud est sous tension. • **Inactif** : le nœud n'est pas sous tension ou connecté.
Province	Le champ **State** (État) indique l'état d'appartenance à la grappe du nœud. Les valeurs possibles sont les suivantes : • **Nouveau** : le nœud ne fait pas encore partie de la grappe. • **Initialisé** : le nœud fait partie de la grappe. Cependant, Cisco Secure Workload n'est pas déployé sur le nœud. • **Mis en service** : le nœud est opérationnel et fonctionne sur Cisco Secure Workload. Le champ de version logicielle est également indiqué et devient rouge si un nœud individuel n'a pas la même version que celle de l'ensemble de la grappe. • **Désactivé** : le nœud a été supprimé de la grappe à des fins de dépannage. Le nœud doit être remplacé par du nouveau matériel. Un nœud peut être désactivé à l'aide de l'action de mise hors-service (voir les actions suivantes).
Port de commutation	Désigne le port de commutateur des deux commutateurs sur lesquels le nœud physique est connecté.
Disponibilité	Indique la durée pendant laquelle le nœud a fonctionné sans redémarrage ni arrêt.

Champ	Description
Instantanés du contrôleur CIMC	Peuvent être utilisés pour lancer une collecte d'assistance technique du contrôleur CIMC et télécharger un fichier d'assistance technique du contrôleur CIMC.

Table 39: Actions correctives de la grappe

Action	Description
Mise en service	Sélectionnez cette action pour intégrer de nouveaux nœuds dans la grappe. Seuls les nœuds avec l'état Nouveau peuvent être sélectionnés pour cette action.
Mise hors service	Sélectionnez cette action pour supprimer les nœuds qui font partie de la grappe. Seuls les nœuds avec l'état **Mise en service** ou **Initialisé** peuvent être sélectionnés pour cette action.
Recréation d'image	Sélectionner cette action pour redéployer Cisco Secure Workload. Cela peut effacer toutes les données de la grappe et est particulièrement utile pour la mise à niveau d'une machine sans système d'exploitation à partir d'une version antérieure vers une nouvelle. Cette étape est requise lors de la désactivation d'une machine sans système d'exploitation.
Mise à niveau du micrologiciel	Les informations sur le micrologiciel sont disponibles pour les nœuds pour lesquels l'adresse IP du contrôleur CIMC est accessible. Cette action est utile pour mettre à niveau le micrologiciel sur les nœuds avec des versions plus anciennes.
Mettre hors tension	Sélectionnez cette action pour mettre les nœuds hors tension. **Note** Vous ne pouvez pas mettre hors tension les nœuds avec l'état **Inactive** (Inactif) et **Shutdown in progress** (Arrêt en cours).

Détails des mises à niveau du micrologiciel

La grappe Cisco Secure Workload sur site regroupe un système informatique unifié (UCS) Cisco Integrated Management Controller (CIMC) Host Upgrade Utility (HUU) ISO. L'option de mise à niveau du micrologiciel sur la page d'état de la grappe peut être utilisée pour mettre à jour une version physique sans système d'exploitation vers la version du micrologiciel UCS incluse dans l'image HUU ISO qui a été groupée dans les RPM Cisco Secure Workload.

La mise à jour du micrologiciel peut commencer sur un hôte sans système d'exploitation lorsque l'état est *actif* ou *inactif* , tant que l'état sans système d'exploitation n'est pas *initialisé* ou *Incompatibilité UGS*. Un

seul micrologiciel UCS à la fois peut voir son micrologiciel UCS mis à jour. Pour démarrer la mise à jour du micrologiciel, l'état Cisco Secure Workload de l'orchestrateur doit être *Idle* (inactif). Lorsque la mise à jour du micrologiciel UCS est lancée, certaines des fonctionnalités de l'interface utilisateur spécifiques à la page d'état de la grappe peuvent être temporairement touchées si le consul leader, l'orchestration ou le gestionnaire actif du micrologiciel (fwmgr) doit être commuté vers d'autres hôtes - ces basculements devraient se produire automatiquement . Pendant la mise à jour du micrologiciel, les détails du micrologiciel du système sans système d'exploitation mis à jour ne s'afficheront pas. Après la mise à jour, cela peut prendre jusqu'à 15 minutes avant que les détails du micrologiciel ne s'affichent à nouveau dans la page Cluster Status (État de la grappe). Avant de commencer la mise à jour du micrologiciel, consultez la page Service Status (État des services) pour vérifier que tous les services sont intègres.

Lorsque vous lancez une mise à jour de micrologiciel sur un système sans système d'exploitation, fwmgr vérifie que la mise à jour peut se poursuivre, met hors tension normalement le système sans système d'exploitation si nécessaire, puis se connecte au contrôleur CIMC sur l'environnement sans système d'exploitation et démarre la mise à jour du micrologiciel basée sur HUU. Ce processus de mise à jour du micrologiciel basé sur HUU implique de démarrer le matériel sans système d'exploitation dans HUU ISO, d'effectuer la mise à jour, de redémarrer le contrôleur CIMC pour activer le nouveau micrologiciel, puis de redémarrer la machine sans système d'exploitation dans HUU ISO pour vérifier que la mise à jour a été effectuée. Le processus global de mise à jour peut prendre plus de 2 heures pour un G1 sans système d'exploitation ou plus d'une heure pour un G2 sans système d'exploitation. Lorsque le processus de mise à jour du micrologiciel est lancé, la page Service Status (État du service) peut indiquer que certains services ne sont pas intègres, car les systèmes sans système d'exploitation et toutes les machines virtuelles fonctionnant sur ces services sans système d'exploitation ne sont plus actifs dans la grappe. Lorsque la mise à jour du micrologiciel est terminée, cela peut prendre 30 minutes de plus pour que le système sans système d'exploitation redevienne actif dans la grappe, et il faudra peut-être plus de temps pour que tous les services soient de nouveau intègres. Si les services ne récupèrent pas dans les deux heures suivant une mise à jour du micrologiciel, contactez un représentant du service d'assistance à la clientèle.

Vous pouvez cliquer sur un nœud sans système d'exploitation dans la page Cluster Status (État de la grappe) pour développer les détails de ce nœud. Lorsqu'une mise à jour du micrologiciel est lancée, vous pouvez cliquer sur le bouton *View Firmware Upgrade Logs* (Afficher les journaux de mise à niveau du micrologiciel) pour afficher l'état de la mise à jour du micrologiciel. Le journal contient l'état général de la mise à jour du micrologiciel. L'état peut être :

- **La mise à jour du micrologiciel a été déclenchée** : la mise à jour du micrologiciel a été demandée, mais n'a pas encore commencé. Pendant cet état, fwmgr vérifiera que les services requis pour la mise à jour du micrologiciel sont fonctionnels et que le CIMC peut accéder à ces services.
- **La mise à jour du micrologiciel est en cours d'exécution** : la mise à jour du micrologiciel a été lancée. Lorsqu'une mise à jour de micrologiciel atteint cet état, le contrôleur CIMC et HUU contrôlent la mise à jour, et la grappe Cisco Secure Workload signale l'état que lui fournit CIMC au sujet de la mise à jour.
- **La mise à jour du micrologiciel a expiré** : cela indique qu'un processus de mise à jour du micrologiciel a dépassé le délai attendu. Le processus global de mise à jour du micrologiciel a une limite de 240 minutes lorsqu'il entre dans la phase *de mise à jour du micrologiciel en cours* . Pendant la mise à jour du micrologiciel, CIMC peut devenir inaccessible lors du redémarrage avec la nouvelle version, cet état inaccessible a un délai de 40 minutes avant que la mise à jour du micrologiciel ne soit déclarée expirée. Lorsque la mise à jour du micrologiciel a commencé, la surveillance de cette mise à jour expire après 120 minutes.
- **La mise à jour du micrologiciel a échoué avec une erreur** : ceci indique qu'une erreur est survenue et que la mise à jour du micrologiciel a échoué. Le contrôleur CIMC ne donne généralement pas d'indication de réussite ou d'échec, donc cet état indique généralement qu'une erreur s'est produite avant que la mise à jour du micrologiciel ne soit en cours d'exécution.

- **Fin de la mise à jour du micrologiciel** : la mise à jour du micrologiciel s'est terminée sans erreur ni délai d'expiration. Le contrôleur CIMC ne donne généralement pas d'indication de réussite ou d'échec, il est préférable de vérifier que les versions du micrologiciel UCS sont mises à jour lorsque ces détails deviennent disponibles dans la page Cluster Status (État de la grappe) - cela peut prendre jusqu'à 15 minutes pour que ces détails soient disponibles.

Sous l'état général dans la fenêtre contextuelle *View Firmware Upgrade Logs* (afficher les journaux de mise à niveau du micrologiciel) se trouve une section de *progression de la mise à jour* qui contiendra des messages de journal horodatés indiquant la progression de la mise à jour du micrologiciel. Lorsque l'état de *redémarrage de l'hôte en cours* est affiché dans ces messages de journal, CIMC contrôle la mise à jour et la grappe la surveille. La plupart des messages de journal suivants proviennent directement du CIMC et ne sont ajoutés à la liste des messages de journal que si l'état de la mise à jour change.

Sous la section de *progression de la mise à jour* de la fenêtre contextuelle *View Firmware Upgrade Logs* (Afficher les journaux de mise à jour du micrologiciel), une section *Component update status* (État de mise à jour des composants) s'affichera lorsque CIMC commencera à fournir des états de mise à jour de composant individuel. Cette section résume l'état de la mise à jour des divers composants UCS sur le système sans système d'exploitation.

Sauvegarde et restauration des données

La sauvegarde et la restauration des données sont un mécanisme de reprise après sinistre qui copie les données de la grappe Cisco Secure Workload, des connecteurs et des orchestrateurs externes vers un stockage hors site. En cas de sinistre, les données sont restaurées à partir du stockage hors site vers une grappe de même type de taille. Vous pouvez également basculer entre différents sites de sauvegarde.

- La sauvegarde et la restauration des données sont prises en charge pour les grappes physiques de 8 et 39 RU.
- Les données peuvent être sauvegardées dans n'importe quel stockage d'objets externe compatible avec l'API S3V4.
- Cisco Secure Workload nécessite une bande passante et un stockage suffisants pour sauvegarder les données. Des vitesses de réseau lentes et une latence élevée peuvent faire échouer les sauvegardes.
- Les limites de stockage des données sont basées sur le type de sauvegarde sélectionné.
  - Pour la sauvegarde de données en mode continu, nous vous recommandons de stocker 200 To pour les sauvegardes complètes, y compris les données de flux. Pour déterminer l'espace de stockage réel requis, utilisez l'option du **planificateur de capacité** disponible sur la page de sauvegarde des données. Pour en savoir plus, consultez Utiliser le Planificateur de capacité, on page 720. Le manque d'espace de stockage pour de multiples sauvegardes entraîne la suppression fréquente d'anciennes sauvegardes afin de pouvoir gérer les sauvegardes dans la limite de l'espace de stockage. Il doit y avoir suffisamment de stockage pour au moins une sauvegarde.
  - Pour la sauvegarde des données en mode continu, le stockage minimal requis est de 50 To pour les sauvegardes complètes, y compris les données de flux. Pour déterminer l'espace de stockage réel requis, utilisez l'option du **planificateur de capacité** disponible sur la page de sauvegarde des données. Pour en savoir plus, consultez Utiliser le Planificateur de capacité, on page 720. Le manque d'espace de stockage pour de multiples sauvegardes entraîne la suppression fréquente d'anciennes sauvegardes afin de pouvoir gérer les sauvegardes dans la limite de l'espace de stockage. Il doit y avoir suffisamment de stockage pour au moins une sauvegarde.

- Pour les sauvegardes en mode allégé, 1 To de stockage est suffisant, car les données de flux, qui constituent la majeure partie des données de sauvegarde, ne sont pas incluses dans la sauvegarde.

- Les données peuvent uniquement être restaurées dans une grappe de taille compatible, exécutant la même version que la grappe principale. Par exemple, vous pouvez restaurer les données d'une grappe de 8 RU uniquement vers une autre de 8 RU.

Sauvegarde des données

Un calendrier pour la sauvegarde des données peut être configuré à l'aide de la section Sauvegarde des données de l'interface utilisateur. Les sauvegardes sont déclenchées une fois par jour et à l'heure programmée en fonction des paramètres configurés ou peuvent être configurées pour s'exécuter en continu. Une sauvegarde réussie s'appelle un *point de contrôle*. Un point de contrôle est un instantané à un point dans le temps des magasins de données principaux de la grappe.

Un point de contrôle réussi peut être utilisé pour restaurer les données sur une autre grappe ou au sein de la même grappe.

Les données de configuration de la grappe sont toujours sauvegardées pour chaque point de contrôle. Le flux et d'autres données constituent la majeure partie des données sauvegardées. Par conséquent, si elles sont configurées correctement, seules les modifications incrémentielles sont sauvegardées. Les sauvegardes incrémentielles permettent de réduire la quantité de données transférées vers le stockage externe, ce qui évite de surcharger le réseau. Si vous le souhaitez, une sauvegarde complète peut être déclenchée selon une planification convenue pour toutes les sources de données lorsque la sauvegarde incrémentielle est configurée. Une sauvegarde complète copie chaque objet d'un point de contrôle, même s'il est déjà copié et que l'objet n'a pas été modifié. Cela peut ajouter une charge importante sur la grappe, sur le réseau entre la grappe et la bibliothèque d'objets, et sur la bibliothèque d'objets elle-même. Une sauvegarde complète peut s'avérer nécessaire en cas de détérioration des objets ou de défaillance matérielle irrémédiable de la bibliothèque d'objets. En outre, si le compartiment fourni pour la sauvegarde change, une sauvegarde complète est automatiquement appliquée, car une sauvegarde complète est nécessaire pour que les sauvegardes incrémentielles soient utiles.

Table 40: Données de grappe sauvegardées dans différents modes

Données de grappe Cisco Secure Workload	Les données sont-elles sauvegardées en mode de sauvegarde complète?	Les données sont-elles sauvegardées en mode allégé?
Configurations de grappe	**Oui**	**Oui**
RPM utilisés pour la création d'image de la grappe	**Oui**	**Oui**
Images de déploiement d'agents logiciels	**Oui**	**Oui**
Base de données de flux	**Oui**	Non
Données requises pour la découverte automatique des politiques	**Oui**	Non

Données de grappe Cisco Secure Workload	Les données sont-elles sauvegardées en mode de sauvegarde complète?	Les données sont-elles sauvegardées en mode allégé?
Données pour faciliter la criminalistique, comme les condensés de fichiers et les modèles de fuites de données.	**Oui**	Non
Données pour faciliter l'analyse de la surface d'attaque	**Oui**	Non
Bases de données CVE.	**Oui**	Non

Note

- Les informations du connecteur sécurisé ne sont pas sauvegardées ou restaurées dans la version sur site de Cisco Secure Workload, mais sont sauvegardées et restaurées dans la version logiciel-service (SaaS) de Cisco Secure Workload.
- Les informations sur les correctifs virtuels des connecteurs FMC ne sont pas restaurées après la restauration des données sauvegardées.

Pre-Requisites for Data Backup

- To obtain an activation key for the Data Backup and Restore (DBR) feature, send an email to taentitlement@cisco.com requesting a DBR activation key and also attach the cluster ID file in the email.

Note The license entitlement is only required for the primary (active) cluster and not by the standby cluster.

- The access and secret keys for the object store are required. The Data backup and restore option does not work with pre-authenticated link for object store.
- Configure any policing to throttle the bandwidth used by the Secure Workload appliance to object store. Note that policing with low bandwidth when volume of data to be backed up is high can cause backup failures.
- Configure the cluster's FQDNs and ensure that software agents can resolve the FQDNs.

Note After you enable data backup and restore, only the current and later software agent versions are available for installation and upgrades. Earlier versions than the current cluster version remain hidden due to incompatibility.

Software agent or Kafka FQDNs Requirements

Software agents use an IP address to get control information from Secure Workload appliance. To enable data backup and restore and allow for seamless failover after a disaster, agents must switch to using FQDN.

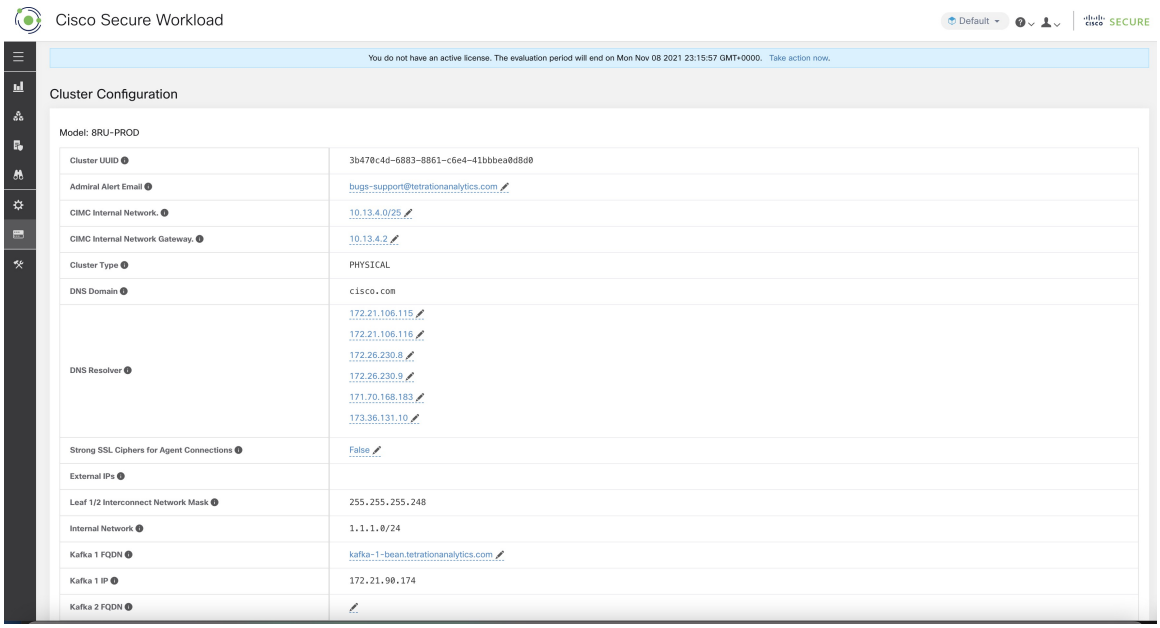
Upgrading Secure Workload cluster is not sufficient for this switch. Software agents support the use of FQDN starting Secure Workload version 3.3 and later. Therefore, to enable agent failover and to ensure that agents are ready for data backup and restore, upgrade the agents to version 3.3 or later.

If FQDNs are not configured, the default FQDNs are:

IP Type	Default FQDN
Sensor VIP	wss{{cluster_ui_fqdn}}
Kafka 1	kafka-1-{{cluster_ui_fqdn}}
Kafka 2	kafka-2-{{cluster_ui_fqdn}}
Kafka 3	kafka-3-{{cluster_ui_fqdn}}

The FQDNs can be changed on the **Platform** > **Cluster Configuration** page.

Figure 426: FQDNs or IP for Data Backup and Restore on Cluster Configuration page



Update the DNS record for the FQDNs with the IPs provided in the same page. The following table lists the mapping of IPs and FQDNs.

Field Name	Corresponding IP Field	Description
Sensor VIP FQDN	Sensor VIP	Update the FQDN to connect to cluster control plane
Kafka 1 FQDN	Kafka 1 IP	Kafka node 1 IP
Kafka 2 FQDN	Kafka 2 IP	Kafka node 2 IP
Kafka 3 FQDN	Kafka 3 IP	Kafka node 3 IP

Note FQDN for sensors VIP and Kafka hosts can only be changed before data backup and restore is configured. After the configuration, FQDN cannot be changed.

Exigences du magasin d'objets

La boutique d'objets doit fournir une interface de plainte S3V4.

Note Quelques stockages d'objets conformes à S3V4 ne prennent pas en charge la fonctionnalité DeleteObjects (SupprimerObjets). La fonctionnalité DeleteObjects est requise pour supprimer les informations de point de contrôle obsolètes. L'absence de cette fonctionnalité peut entraîner des échecs lors de la tentative de suppression des points de contrôle obsolètes du stockage et peut entraîner un manque d'espace du stockage.

- **Site**

  L'emplacement du magasin d'objets est essentiel pour la latence liée à la sauvegarde et à la restauration du magasin. Pour améliorer le temps de restauration, vérifiez que le magasin d'objets est situé plus près de la grappe de secours.

- **Compartiment**

  Créez un nouveau compartiment dédié à Cisco Secure Workload dans le magasin d'objets. Seule la grappe doit avoir un accès en *écriture* à ce compartiment. La grappe écrira les objets et gérera la rétention sur le compartiment. Mettez en service au moins 200 To de stockage pour le compartiment et obtenez un accès et une clé secrète pour ce dernier. La sauvegarde et la restauration des données dans Cisco Secure Workload ne fonctionnent pas avec les liens pré-authentifiés.

Note Si vous utilisez Cohesity comme magasin d'objets, désactivez les chargements en plusieurs parties lors de la planification.

- **HTTPS**

  L'option de sauvegarde de données prend uniquement en charge l'interface HTTPS avec le magasin d'objets. Cela permet de s'assurer que les données en transit vers ce dernier sont chiffrées et sécurisées. Si le certificat de stockage SSL/TSL est signé par une autorité de certification tierce de confiance, la grappe l'utilisera pour authentifier le magasin d'objets. Si le magasin d'objets utilise un certificat autosigné, la clé publique ou l'autorité de certification peut être téléversée en sélectionnant l'option **Use Server CA Certificate** (Utiliser le certificat de l'autorité de certification du serveur).

- **Chiffrement côté serveur**

  Il est fortement recommandé d'activer le chiffrement côté serveur pour le compartiment affecté à la grappe de Cisco Secure Workload. La grappe utilisera HTTPS pour transférer les données vers le magasin d'objets. Cependant, le magasin d'objets doit chiffrer les objets pour s'assurer que les données stockées sont sécurisées.

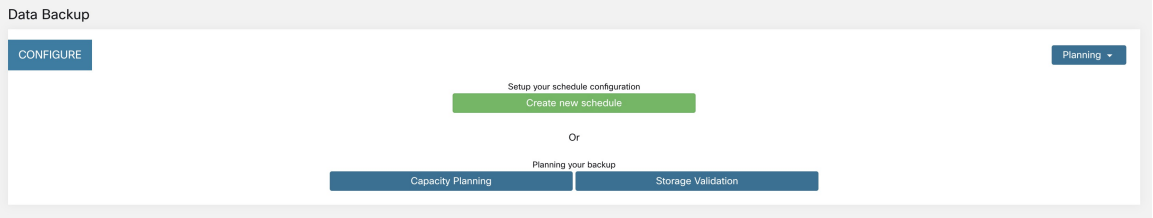
Configuration of Data Backup

To configure data backup in Secure Workload, perform the following:

1. **Planning**—The data backup option provides a planner to test the access to the object store, determine the storage requirement, and the backup duration needed for each day. This can be used to experiment before configuring a schedule.

   To use data backup and restore calculators, navigate to **Platform** > **Data Backup**. If data backup and restore is not configured, this will navigate to the Data Backup landing page.

   Figure 427: Backup Landing Page

   - Utiliser le Planificateur de stockage, on page 719
   - Utiliser le Planificateur de capacité, on page 720

   Note If you are unable to view the Data Backup option under Platform, ensure that you have the license to enable data backup and restore.

2. **Configuring and scheduling data backup**—Secure Workload will copy data to object store only in the configured time-window. While configuring backup for the first time, the pre-checks will run to ensure the FQDNs are resolvable and resolves to the right IP. After the initial validation, an update is pushed to registered software agents to switch to using FQDNs. Without FQDN, the agents cannot failover to another cluster after a disaster event. To support this, agents must be upgraded to the latest version supported by the cluster and all the agents should be able to resolve the sensor VIP FQDN. As of Secure Workload release 3.3 and later, only deep visibility and enforcement agents support data backup and restore and will switch to using FQDN.

   To create a schedule and configure data backup, see Configurer la sauvegarde des données, on page 721.

Utiliser le Planificateur de stockage

Procedure

Étape 1 Pour vous assurer que le stockage est compatible avec Cisco Secure Workload, effectuez l'une des actions suivantes :

- Dans la page de destination de la **sauvegarde des données**, cliquez sur **Storage Planning**(planification du stockage).
- Dans le menu déroulant **Planning** (Planification), choisissez **Storage**(stockage).

La page **Storage Planning** (planification du stockage) s'affiche.

Étape 2 Saisissez les informations suivantes :

- Un nom pour le stockage.
- URL d'un point terminal de stockage conforme à S3.

  Note L'adresse IPv6 d'un stockage conforme S3 doit être une URL ou un nom de domaine complet, et pas seulement une adresse IPv6.

- Un nom de compartiment conforme à S3 configuré sur le stockage
- (Facultatif pour certains types de stockage) Région du stockage conforme à S3.
- Clé d'accès au stockage.
- Clé secrète du stockage.

Étape 3 (Facultatif) Si nécessaire, vous pouvez activer le serveur mandataire HTTP.

Étape 4 (Facultatif) Pour utiliser des chargements en plusieurs parties des données sauvegardées, activez **Use Multipart Upload**(utiliser le chargement en plusieurs parties) .

Étape 5 (Facultatif) Si un certificat de l'autorité de certification est requis pour authentifier le serveur de stockage, activez l'option **Use Server CA Certificate** (utiliser le certificat de l'autorité de certification du serveur) et saisissez les détails du certificat.

Étape 6 Cliquez sur **Test**.

La validation du stockage permet de tester :

- L'authentification et l'accès au magasin d'objets et au compartiment.
- Le téléchargement vers et depuis le compartiment configuré.
- Les vérifications de la bande passante.

Le processus de planification du stockage peut prendre environ cinq minutes.

Utiliser le Planificateur de capacité

Procedure

Étape 1 Pour planifier la taille de stockage et les estimations de la fenêtre de sauvegarde, effectuez l'une des actions suivantes :

- Dans la page de destination de **Data Backup** (sauvegarde des données), cliquez sur **Capacity Planning** (Planification de la capacité).
- Dans le menu déroulant **Planning** (Planification), choisissez **Capacity**(capacité).

La page **Planification de la capacité** s'affiche.

Étape 2 Saisissez la limite de bande passante maximale pour sauvegarder les données.

Cette bande passante doit au plus correspondre à la configuration du contrôleur qui limitera les données envoyées au magasin d'objets.

Étape 3 Le nombre d'agents logiciels enregistrés est rempli automatiquement. En fonction des prévisions, vous pouvez modifier le nombre d'agents.

Étape 4 (Facultatif) Activez **Lean Data Mode** (le mode de données allégé) pour exclure les données qui ne font pas partie de la configuration de la sauvegarde. L'utilisation de cette option réduit la limite de stockage de 75 %.

Étape 5 Le stockage maximal configuré pour l'ensemble de stockage. Cela définira automatiquement la période de rétention des sauvegardes.

Une fois les renseignements détaillés requis saisis, la durée estimée de la sauvegarde affiche le temps requis pour la sauvegarde des données d'une journée. Il s'agit d'une estimation basée sur la charge d'agent typique, le nombre d'agents estimatif et la bande passante maximale configurée. L'estimation de la capacité de stockage maximale affiche l'estimation de la capacité de stockage maximale requise par Cisco Secure Workload pour prendre en charge la rétention précisée et le nombre estimatif d'agents.

Configurer la sauvegarde des données

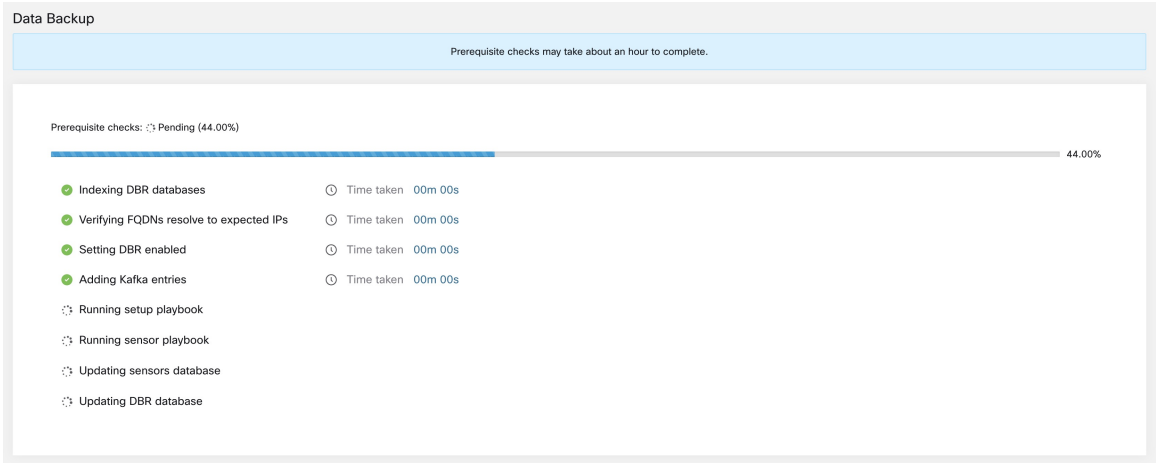
Procedure

Étape 1 Dans la page de destination de la sauvegarde des données, cliquez sur **Create new schedule** (Créer une nouvelle planification).

Étape 2 Pour confirmer les vérifications des préalables à exécuter, cochez les boutons **Approve** (approuver) et cliquez sur **Proceed** (Continuer).

La vérification des préalables prend environ 30 minutes et n'est exécutée que lors de la première configuration d'une planification.

Figure 428: Exécution de la sauvegarde des conditions préalables



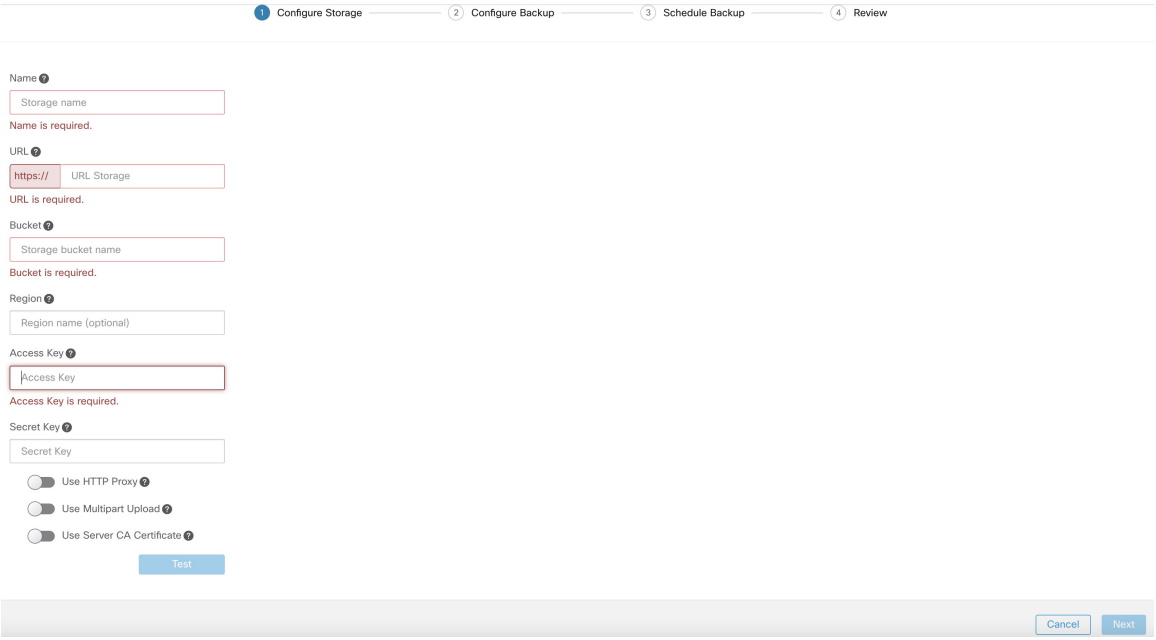
Étape 3 Pour configurer le stockage, entrez les détails suivants et cliquez sur **Test** (Tester).

- Un nom pour le stockage.
- URL d'un point terminal de stockage conforme à S3.

Note L'adresse IPv6 d'un stockage conforme S3 doit être une URL ou un nom de domaine complet, et pas seulement une adresse IPv6.

- Un nom de compartiment conforme à S3 configuré sur le stockage
- (Facultatif pour certains types de stockage) Région du stockage conforme à S3.
- Clé d'accès au stockage.
- Clé secrète du stockage.
- (Facultatif) Activez le serveur mandataire HTTP, si nécessaire.
- (Facultatif) Pour utiliser des chargements en plusieurs parties des données sauvegardées, activez **Use Multipart Upload**(utiliser le chargement en plusieurs parties) .
- (Facultatif) Si un certificat de l'autorité de certification est requis pour authentifier le serveur de stockage, activez l'option **Use Server CA Certificate** (utiliser le certificat de l'autorité de certification du serveur) et saisissez les détails du certificat.

Figure 429: Configuration du stockage.

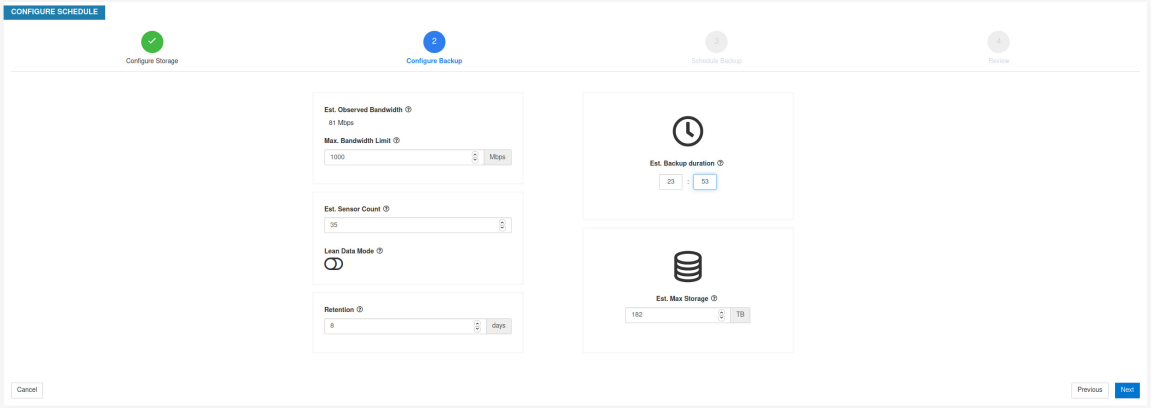


Étape 4 Pour configurer la capacité de stockage, saisissez les informations suivantes :

- La limite de bande passante maximale pour la sauvegarde des données. Cette bande passante doit au plus correspondre à la configuration du contrôleur qui limitera les données envoyées au magasin d'objets.
- Le nombre d'agents logiciels enregistrés est rempli automatiquement. En fonction des prévisions, vous pouvez modifier le nombre d'agents.
- (Facultatif) Activez **Lean Data Mode** (le mode de données allégé) pour exclure les données qui ne font pas partie de la configuration de la sauvegarde. L'utilisation de cette option réduit la limite de stockage de 75 %.

- Le stockage maximal configuré pour l'ensemble de stockage. Cela définira automatiquement la période de rétention des sauvegardes.

Figure 430: Planification de la capacité



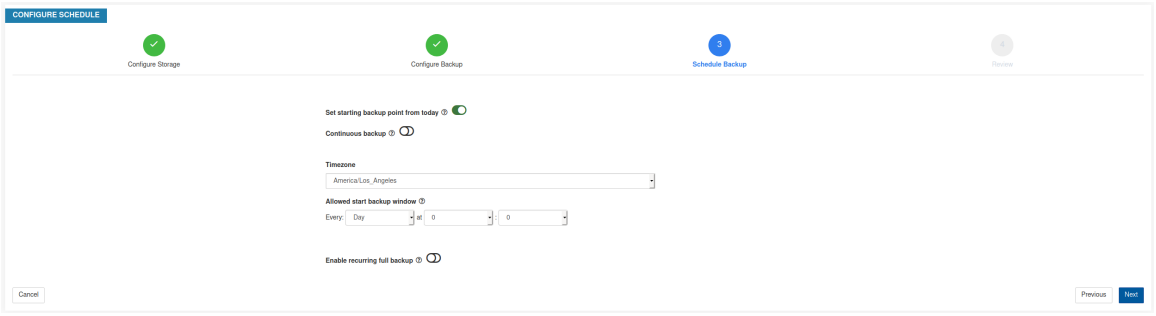
Étape 5 Pour planifier la sauvegarde, activez les éléments suivants :

- Par défaut, l'option **Set starting backup point from today** (Définir le point de sauvegarde de départ à partir d'aujourd'hui) est activée. Cette option ignorera tous les fichiers créés avant minuit UTC le jour de la configuration. Dans une grappe qui fonctionne, il peut y avoir un volume élevé de données à sauvegarder le premier jour et qui risque de surcharger la grappe, le réseau et le magasin d'objets. Si vous souhaitez sauvegarder toutes les données existantes, décochez cette case mais notez l'incidence sur le réseau, le magasin d'objets et la grappe.

  Note Toutes les données de configuration seront sauvegardées, quelle que soit cette option.

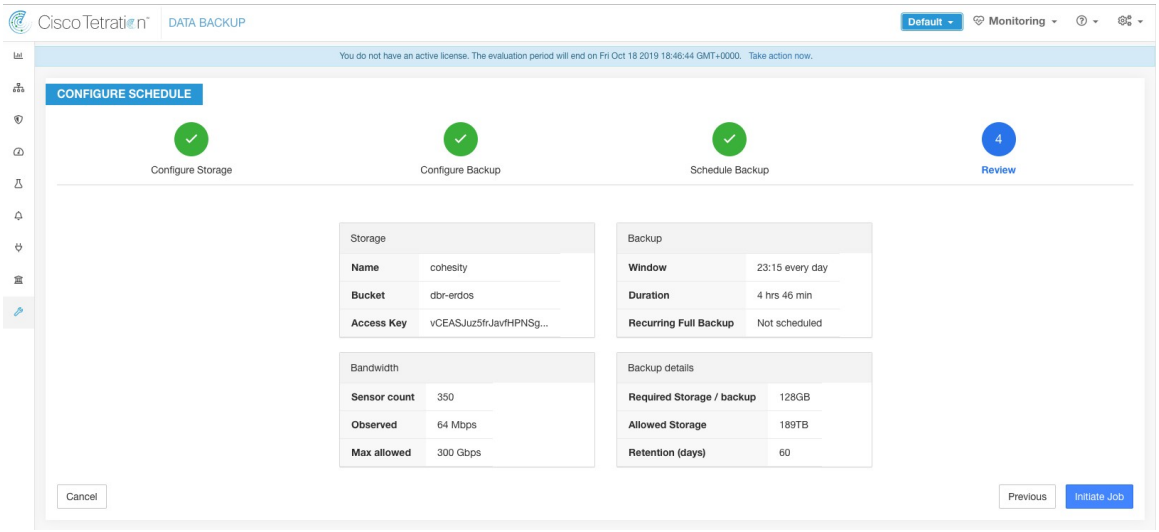
- Sauvegarde continue : si cette option est activée, les données seront sauvegardées 15 minutes après la fin de la sauvegarde précédente. Cette option permet aux sauvegardes de s'exécuter en permanence, au lieu d'être planifiées à une heure précise. Les options de **fuseau horaire** et **de fenêtre de sauvegarde de début autorisée** ne sont pas disponibles lorsque la sauvegarde continue est activée.
- Les deux options suivantes sont utilisées pour configurer la planification de la sauvegarde, si la sauvegarde en continu n'est pas utilisée.
  - Time zone (Fuseau horaire) : utilise par défaut le fuseau horaire du navigateur Web
  - Allowed Start save Window (fenêtre autorisée de démarrage de la sauvegarde) : heure (en heures ou minutes) à laquelle la sauvegarde commencera. L'heure doit être saisie au format 24 heures
  - Activer la sauvegarde complète récurrente (non sélectionnée par défaut) : Si cette option est activée, une planification pour la sauvegarde complète peut être configurée. Par défaut, après la première sauvegarde complète, toutes les sauvegardes sont différentielles. L'activation de cette configuration forcera une sauvegarde complète selon le calendrier spécifié.

Figure 431: Planifier une sauvegarde



Étape 6 Passez en revue la planification et les paramètres de sauvegarde configurés, puis cliquez sur **Initiate Job** (Démarrer a tâche).

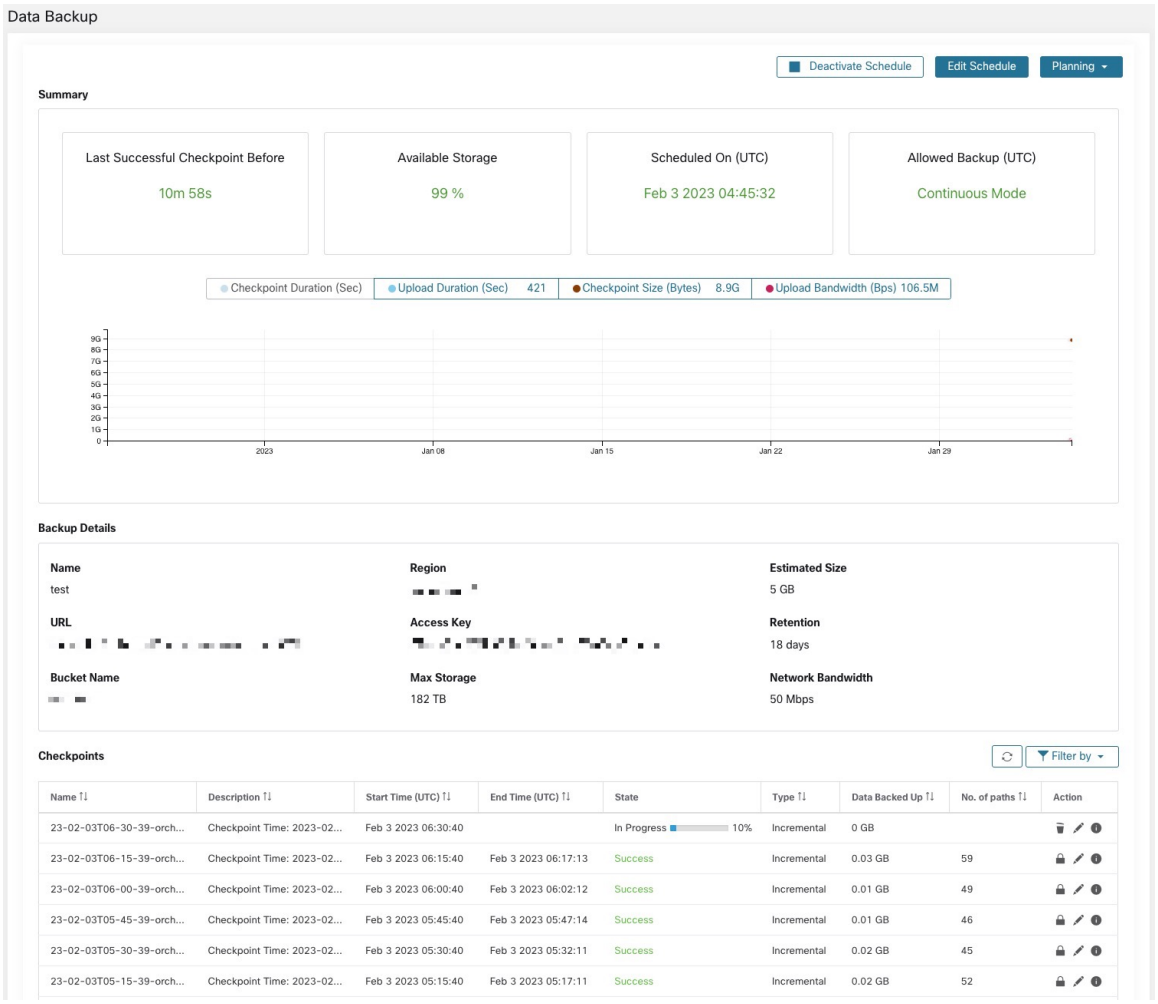
Figure 432: Examiner la configuration de sauvegarde)



État de la sauvegarde

Après la configuration de la sauvegarde des données, elle est déclenchée tous les jours à une heure planifiée, sauf si le mode continu est activé. L'état des sauvegardes peut être consulté sur le tableau de bord de la sauvegarde des données en accédant à **Platform (Plateformes)** > **Data Backup (Sauvegarde des données)**.

Figure 433: État de la sauvegarde



Le temps écoulé depuis le dernier point de contrôle réussi doit être inférieur à 24 heures + le temps nécessaire au point de contrôle. Par exemple, si le point de contrôle + la sauvegarde prennent environ 6 heures, le temps écoulé depuis le dernier point de contrôle réussi doit être inférieur à 30 heures.

Les graphiques suivants fournissent des renseignements supplémentaires :

- Durée du point de contrôle : ce graphique montre la ligne de tendance de la durée du point de contrôle.
- Durée du chargement : ce graphique montre la ligne de tendance pour le temps nécessaire au chargement du point de contrôle vers la base de données de sauvegarde.
- Taille du point de contrôle : ce graphique montre la ligne de tendance pour la taille du point de contrôle.
- Bande passante de téléversement : ce graphique montre la ligne de tendance de la bande passante de téléversement.

Le tableau présente tous les points de contrôle. Les étiquettes de point de contrôle peuvent être modifiées et seront disponibles lors du choix d'un point de contrôle pour restaurer les données sur la grappe de secours.

Un point de contrôle passe par plusieurs états. Voici les états possibles :

- Créé/en attente : le point de contrôle vient d'être créé et en attente de copie.
- En cours d'exécution : les données sont sauvegardées activement sur un stockage externe
- Réussite : le point de contrôle est terminé et a réussi; peut être utilisé pour la restauration des données
- Échec : le point de contrôle est terminé et a échoué; ne peut pas être utilisé pour la restauration des données
- Suppression en cours/Supprimé : un point de contrôle obsolète est en cours de suppression ou est supprimé

Pour modifier la planification ou le regroupement, cliquez sur **Edit Schedule** (Modifier le calendrier). Pour terminer la mise en œuvre de l'assistant, consultez la section Configurer la sauvegarde des données.

Pour résoudre les erreurs lors de la création des points de contrôle, consultez Dépannage : sauvegarde et restauration des données, on page 733.

Désactiver la planification de sauvegarde

Les sauvegardes peuvent être désactivées en cliquant sur le bouton **Deactivate Schedule** (Désactiver la planification). Il est recommandé de désactiver la planification de sauvegarde avant d'y apporter des modifications. Désactivez la planification uniquement lorsqu'aucun point de contrôle n'est en cours. L'exécution d'un test ou la désactivation de la planification alors qu'un point de contrôle est en cours peut entraîner l'échec de ce dernier et un état indéfini du téléchargement.

Rétention du magasin d'objets

La grappe Cisco Secure Workload gère le cycle de vie des objets du compartiment. Vous ne devez pas supprimer ni ajouter d'objets au compartiment. Cela pourrait entraîner des incohérences et endommager les points de contrôle réussis. Dans l'assistant de configuration, la mémoire maximale à utiliser doit être spécifiée. Cisco Secure Workload fait en sorte que l'utilisation du compartiment ne dépasse pas la limite configurée. Il existe un service de conservation du stockage qui élimine les objets après un certain temps et les supprime du compartiment. Une fois que l'utilisation du stockage a atteint un seuil (80 % de la capacité du compartiment) calculé en fonction du stockage maximal configuré et du débit de données entrantes, la fonction de rétention tente de supprimer les points de contrôle *non conservés* pour ramener l'utilisation sous le seuil. La fonction de rétention conservera également un minimum de deux points de contrôle réussis à tout moment et tous les points de contrôle préservés, le nombre le plus élevé des deux situations étant retenu. Si la fonction de rétention ne peut supprimer aucun point de contrôle pour libérer de l'espace, les ***points de contrôle commenceront à générer des échecs***.

Conserver les points de contrôle

À mesure que de nouveaux points de contrôle sont créés, les anciens expirent et sont supprimés. Cependant, les points de contrôle peuvent être conservés, empêchant ainsi leur suppression par la fonction de rétention. Un point de contrôle conservé ne sera pas supprimé. S'il y a plusieurs points de contrôle conservés, à un moment donné, le stockage sera insuffisant pour les nouveaux objets et les points de contrôle périmés ne pourront pas être supprimés parce qu'ils ont été conservés. Une bonne pratique consiste à conserver les points de contrôle en fonction des besoins et à mettre à jour l'étiquette du point de contrôle en indiquant la raison et la validité comme référence. Pour conserver un point de contrôle, cliquez sur l'icône représentant un verrou à côté du point de contrôle requis.

Restaurer les données

- Pour restaurer à l'aide de données sauvegardées, une grappe doit être en **mode d'attente DBR**. Actuellement, vous pouvez définir une grappe en mode veille **uniquement lors de la configuration initiale**.
- Une fois que la grappe est en mode veille, choisissez **Platform** (plateforme) dans le volet de navigation pour accéder à l'option de restauration des données.

Cisco Secure Workload prend en charge les combinaisons suivantes :

Table 41: UGS de grappes principale et secondaire pour la restauration des données

UGS de grappe principale	UGS de grappe en attente
8RU-PROD	8RU-PROD, 8RU-M5, 8RU-M6
8RU-M5	8RU-PROD, 8RU-M5, 8RU-M6
39RU-GEN1	39RU-GEN1, 39RU-M5, 39RU-M6
39RU-M5	39RU-GEN1, 39RU-M5, 39RU-M6
8RU-M6	8RU-PROD, 8RU-M5, 8RU-M6
39RU-M6	39RU-GEN1, 39RU-M5, 39RU-M6

UGS de grappe principale	UGS de grappe en attente
8RU-PROD	8RU-PROD, 8RU-M5
8RU-M5	8RU-PROD, 8RU-M5
39RU-GEN1	39RU-GEN1, 39RU-M5
39RU-M5	39RU-GEN1, 39RU-M5

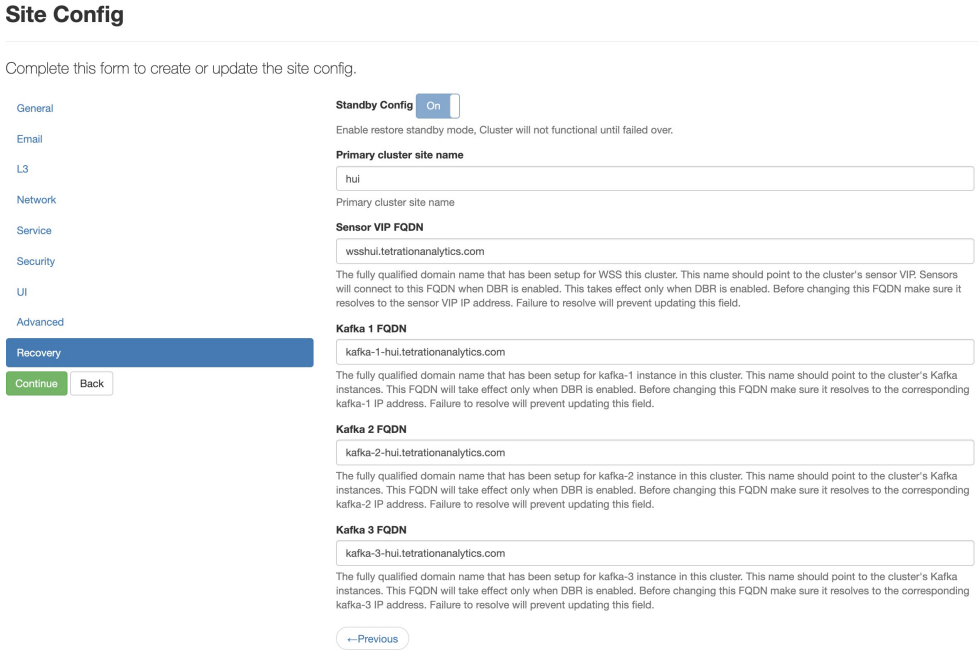
Deploy Cluster in Standby Mode

Contact Cisco to initiate data restore.

A cluster can be deployed in the Standby mode by configuring the recovery options in site information. While configuring site information during deployment, configure the restore details under the **Recovery** tab in the setup UI during deployment.

There are three modes to deploy a standby and for all the three modes, configure these settings:

- Set the **Standby Config** to **On**. This configuration cannot be changed once set until the cluster is redeployed.
- Configure primary cluster name and FQDNs. This configuration can be changed subsequently.



Rest of the deployment is same as a regular deployment of Secure Workload cluster.

A banner is displayed on the Secure Workload UI after the cluster enters the standby mode.

Primary cluster name and FQDNs can be reconfigured after the deployment to enable the standby cluster to track another cluster. This can be reconfigured at a later time before failover is triggered from the Cluster Configuration page.

Standby Deployment Modes

- **Cold Standby**: There is no standby cluster. However, the primary cluster backs the data to S3. During a disaster, a new cluster (or the same cluster as primary) needs to be provisioned, deployed in standby mode and restored.
- **Warm Standby**: A standby cluster is operational and deployed in standby mode. It periodically fetches state from S3 cluster and places it in the ready state to be operational in case of a disaster. During a disaster, log in to this new cluster and trigger a failover.
- **Luke Warm Standby**: Multiple primary clusters are backed by fewer standby clusters. The standby cluster is deployed in standby mode. Only after a disaster, the storage bucket information is configured, data is prefetched, and cluster is restored.

Restore Data to a Secure Workload Cluster

Before you begin

Ensure that the cluster is deployed in standby mode. For more details, see Deploy Cluster in Standby Mode.

Procedure

Étape 1 (Optional) If you have already configured the storage details, go to Step 2. To configure S3 storage, enter the following details:

- A name for the storage.
- The URL of an S3-compliant storage endpoint.

  Note The IPv6 address of an S3-compliant storage must be a URL or FQDN, and not just an IPv6 address.

- An S3-compliant bucket name configured on the endpoint storage.
- (Optional for certain storage) Region of the S3-compliant storage.
- Access key to the storage.
- Secret key of the storage.
- (Optional) Enable HTTP proxy, if necessary.
- (Optional) If a CA certificate is required to authenticate the storage server, enable **Use Server CA Certificate** and enter the certificate details.

Étape 2 Click **Test** to check if the S3 storage is accessible from the Secure Workload cluster.

The status of the tests that are performed are displayed in the table. If there are any errors connecting to the storage, read the description and troubleshoot the errors to continue to the next step.

Étape 3 Click **Next**.

Étape 4 Under **Pre-checks**, the status of the prechecks runs by Secure Workload are displayed. To manually run the prechecks, click **Perform Check**.

The status of all the checks is displayed:

- For the checks that have an error, but do not prevent you from restoring the data, hover your cursor over the warning icon to get the details and a link to navigate to the **Service Status** page to get more details of the service.
- If any of the checks failed, you must troubleshoot the issue to proceed with data restore. Navigate to the **Service Status** page to get more details of the service.

Note Ensure that the checkpoint you are restoring to is the latest with no errors.

Étape 5 Click **Start restore process**.

Under **Restore**, all the data restore jobs that run, the configured S3 storage details, and the status of the data restore prechecks are displayed.

Étape 6 Click **Restore now**.

Étape 7 In the confirmation dialog box, check the check boxes to confirm that you agree to the fact that agent connectivity is lost and data may be lost during the data restore. Click **Confirm** to start the data restore process.

The progress of the data restore process is displayed.

Caution At the **Pre Restore Playbook** stage, all the services within the cluster are reinitialized and there is a downtime of approximately two hours. At this stage, the Secure Workload GUI is not accessible. For more information about the phases that are involved in data restore, see Phases de restauration de la grappe.

If the GUI is rendered inaccessible for an extended period, contact the Cisco Technical Assistance Center to troubleshoot the issue.

Note

After the **Post Restore Playbook** stage, the GUI is accessible and the status of all the jobs are updated. A confirmation message is displayed indicating that the data restore is successful.

What to do next

Update your DNS server to redirect the configured FQDNs to the cluster IP address, which ensures that the software agents communicate with the cluster after the cluster failover is complete.

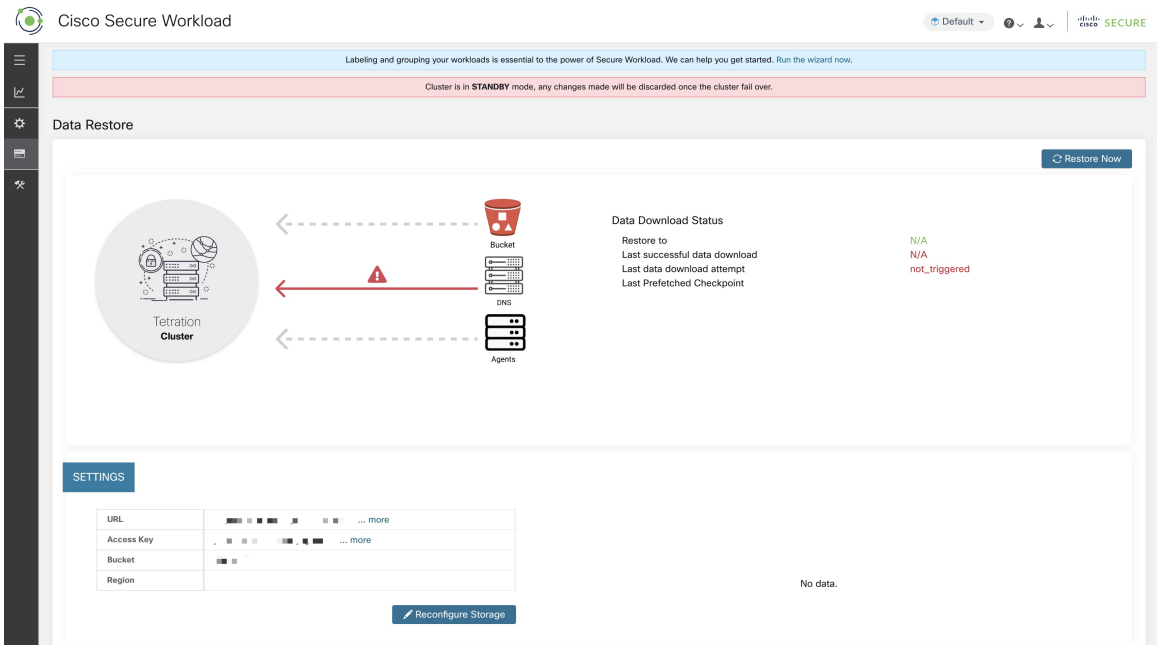
Pré-lecture des données de grappe

Avant de pouvoir restaurer la grappe, elle doit précharger les données. Les données du point de reprise sont prélues à partir du même compartiment de stockage que celui utilisé pour la sauvegarde des données. Des informations d'authentification doivent être fournies pour que le service de sauvegarde puisse être téléchargé à partir du stockage. Si un stockage n'est pas configuré pour la prélecture, l'onglet **Data Restore** (Restauration des données) lance l'assistant de configuration.

Note La grappe de secours interagit uniquement avec le stockage S3. Lorsque la sauvegarde sur la grappe principale est mise à jour pour utiliser un stockage ou un compartiment différent, la grappe de stockage en attente doit être mise à jour.

Une fois les informations validées, le stockage est automatiquement configuré pour la pré-lecture. L'onglet Restaurer affichera l'état de la pré-lecture.

Figure 434: État de la pré-lecture



La page État affiche les éléments suivants :

- La section supérieure gauche comporte un graphique indiquant que les divers composants sont prêts à démarrer une restauration. Pour vérifier les données, survolez avec le curseur les composants. Les données associées s'affichent dans la section supérieure droite.
    - **Compartiment** : affiche l'état de la pré-lecture. Si les dernières données datent de plus de 45 minutes, elles s'affichent en rouge. Notez que les dernières données datant de plus de 45 minutes n'est pas un problème si la sauvegarde sur le périphérique actif prend plus de 45 minutes pour chaque point de contrôle.
    - **DNS** : Affiche les résolutions de nom de domaine complet (FQDN) Kafka et WSS par rapport aux adresses IP des grappes de secours. Pendant la restauration, si les noms de domaine complets ne sont pas mis à jour pour les adresses IP de grappe de secours, l'agent ne peut pas se connecter. Une fois que les noms de domaine complets ont commencé à être résolus vers la grappe de secours, l'état devient vert.
    - **Agents** : affiche le nombre d'agents logiciels qui ont basculé avec succès vers la grappe de secours. Cela n'est pertinent qu'après le déclenchement d'une restauration.
- La section supérieure droite affiche les renseignements pertinents pour le graphique choisi dans la section de gauche. Cliquez sur **Restore Now** (Restaurer maintenant) pour lancer le processus de restauration.
- La section inférieure gauche affiche les paramètres de stockage de prélecture qui sont utilisés.
- La section inférieure droite affiche un graphique des retards de pré-lecture.

Une pré-lecture des données met à jour plusieurs composants nécessaires pour assurer une restauration rapide. Si une pré-lecture de données ne peut pas se terminer, la raison de l'échec est affichée dans la page d'état.

Erreurs courantes qui peuvent entraîner des échecs de pré-lecture :

Erreur d'accès S3 : dans ce cas, les données du stockage n'ont pas pu être téléchargées avec succès. Cela peut se produire en raison de renseignements d'authentification non valides, d'une modification des politiques de stockage ou de problèmes réseau temporaires.

Versions de grappe incompatibles : les données peuvent être restaurées dans une grappe exécutant la même version (y compris la même version de correctif) de Cisco Secure Workload que la grappe principale. Cela peut probablement se produire lors des mises à niveau lorsqu'un seul de la grappe est mis à niveau. Ou, pendant le déploiement, lorsqu'une version différente est utilisée pour le déploiement. Le déploiement des grappes sur une version commune résoudra le problème.

Versions d'UGS incompatibles : notez les UGS autorisées pour les grappes de secours de la grappe principale. Seules des UGS spécifiques sont autorisées pour la restauration de l'UGS de grappe principale.

Phases de restauration de la grappe

Les données de la grappe sont restaurées en deux phases :

- **Phase obligatoire** : Les données nécessaires au redémarrage des services sont restaurées en premier. La durée d'une phase obligatoire dépend de la configuration, du nombre d'agents logiciels installés, de la quantité de données sauvegardées et des métadonnées de flux. Pendant la phase obligatoire, l'interface utilisateur n'est pas accessible. **Des clés d'invité TA fonctionnels sont nécessaires pour toute prise en charge pendant la phase obligatoire, le cas échéant.**
- **Phase de transmission** : les données de la grappe (y compris les données de flux) sont restaurées en arrière-plan et ne bloquent pas l'utilisation de la grappe. L'interface utilisateur de la grappe est accessible et une bannière s'affiche avec le pourcentage de restauration terminée. Pendant cette phase, la grappe est opérationnelle, les pipelines de données fonctionnent normalement et les recherches de flux sont également disponibles.

Une fois la phase obligatoire de la restauration terminée et l'interface utilisateur accessible, les modifications apportées à la grappe doivent être communiquées aux agents logiciels. Dans le serveur DNS utilisé par les agents, l'adresse IP associée au nom de domaine complet de la grappe doit être mise à jour et l'entrée DNS doit pointer vers la grappe restaurée. Une recherche DNS est déclenchée par les agents lorsque la connexion à la grappe principale est interrompue. En fonction de l'entrée DNS mise à jour, les agents se connectent à la grappe restaurée.

Objectif de temps de reprise (RTO) et objectif de point de reprise (RPO)

Cette section décrit l'objectif de temps de récupération (RTO) et l'objectif de point de récupération (RPO) pour la solution de sauvegarde et de restauration des données.

Une sauvegarde lancée sur la grappe principale nécessite un certain temps pour se terminer en fonction de la quantité de données sauvegardées et de la configuration de la sauvegarde. Les différents modes de sauvegarde définissent l'objectif de point de récupération (RPO) de la solution.

- Si elle est planifiée, la sauvegarde non continue est utilisée et est lancée une fois par jour. En cas de sinistre, la durée maximale de perte de données sera d'environ 24 heures, en plus du temps nécessaire pour copier les données dans le stockage de sauvegarde. Par conséquent, l'objectif de point de récupération (RPO) est d'au moins 24 heures.
- Si une sauvegarde en mode continu est utilisée, une nouvelle sauvegarde est lancée 15 minutes après la sauvegarde précédente. Chaque sauvegarde prend un certain temps à créer, puis à téléverser les données vers le stockage de sauvegarde. La première sauvegarde est une sauvegarde complète et les sauvegardes suivantes sont des sauvegardes différentielles , les sauvegardes différentielles ne prennent pas beaucoup

de temps. En cas de sinistre, la quantité de données perdues correspond à la somme du temps nécessaire pour créer la sauvegarde et du temps nécessaire pour téléverser la sauvegarde dans le système de stockage. Dans ce cas, en général, l'objectif de RPO sera d'environ quelques minutes à une heure.

Lors de la restauration d'une grappe, les données obligatoires sont d'abord extraites du stockage, puis la phase de restauration obligatoire est déclenchée. L'interface utilisateur n'est pas disponible pendant la phase de restauration obligatoire. Une fois la restauration obligatoire terminée, l'interface utilisateur est disponible pour utilisation. Le reste des données est restauré lors de la phase de restauration différée. Dans ce cas, le RTO correspond au temps nécessaire jusqu'à ce que l'interface utilisateur soit disponible pour utilisation une fois la phase obligatoire terminée. Les RTO dépendent du mode de déploiement en veille.

- Mode à froid : dans ce mode, la grappe doit d'abord être déployée, ce qui prend environ quelques heures. La grappe doit ensuite être configurée avec les informations d'authentification de stockage de sauvegarde. Comme c'est la première fois que la sauvegarde est téléversée dans la grappe de secours, il y aura beaucoup de données obligatoires qui doivent être récupérées et traitées. La durée de la lecture anticipée est d'environ plusieurs dizaines de minutes (selon la quantité de données sauvegardées). La phase de restauration obligatoire prend environ 30 minutes. L'ensemble forme un temps de RTO d'environ quelques heures, principalement dû au temps nécessaire pour démarrer et déployer la grappe.
- Mode de veille à chaud : dans ce mode, la grappe est déjà déployée, mais le stockage de sauvegarde n'est pas configuré. La grappe doit être configurée avec les informations d'authentification de stockage de sauvegarde. Comme c'est la première fois que la sauvegarde est téléversée dans la grappe de secours, il y aura beaucoup de données obligatoires qui doivent être récupérées et traitées. La durée de la lecture anticipée est d'environ plusieurs dizaines de minutes (selon la quantité de données sauvegardées). La phase de restauration obligatoire prend environ 30 minutes. L'ensemble forme un RTO d'environ une à deux heures, selon la quantité de données sauvegardées et le temps nécessaire pour extraire les données du stockage de sauvegarde.
- Mode de secours immédiat : dans ce mode, la grappe est déjà déployée, le stockage de sauvegarde est configuré et la prélecture récupère les données du stockage. La grappe peut maintenant être restaurée, ce qui déclenchera la phase de restauration obligatoire, qui prend environ 30 minutes. Cela forme le temps RTO d'environ 30 minutes. Notez qu'il s'écoule un certain délai entre le moment où la sauvegarde est téléversée des processus actifs vers le stockage et le moment où la sauvegarde est extraite par la sauvegarde. Ce délai dure environ quelques minutes. Si la dernière sauvegarde du système actif (avant qu'il ne subisse un sinistre) n'a pas été récupérée préalablement sur la sauvegarde, vous devez attendre quelques minutes pour qu'elle soit récupérée.

Mise à niveau avec la sauvegarde et la restauration des données

Lorsque la sauvegarde et la restauration des données sont activées sur la grappe, il est recommandé de désactiver la planification avant de commencer la mise à niveau. Reportez-vous à la section Désactiver la planification de sauvegarde. Cela garantit qu'il existe une sauvegarde réussie avant de commencer la mise à niveau et qu'aucune nouvelle sauvegarde n'est chargée. Une planification doit être désactivée lorsqu'un point de contrôle n'est pas en cours, afin d'éviter la création d'un point de contrôle défaillant.

Dépannage : sauvegarde et restauration des données

Les vérifications de la configuration S3 échouent

Si le test de stockage échoue, identifiez les scénarios de défaillance qui sont affichés dans le volet de droite et vérifiez que :

- L'URL de stockage conforme à S3 est correcte.
- Les clés d'accès et codes secrets du stockage sont corrects.
- Il existe un compartiment de stockage et des autorisations d'accès correctes (lecture/écriture) sont accordées.
- Le serveur mandataire est configuré si le stockage doit être accessible directement.
- L'option de chargement en plusieurs parties est désactivée si vous utilisez Cohesity.

Scénarios d'erreur des vérifications de la configuration S3

Le tableau énumère les scénarios d'erreur courants avec résolution et ne constitue pas une liste exhaustive.

Table 42: Messages d'erreur avec résolution lors de la vérification de la configuration S3

Message d'erreur	Scénario	Résolution
`Introuvable`	Nom de compartiment incorrect	Saisissez le nom correct du compartiment configuré pour le stockage
`Erreur de connexion SSL`	Erreur d'expiration ou de vérification du certificat SSL	Vérifiez le certificat SSL
	URL HTTPS non valide	• Saisissez à nouveau l'URL HTTPS correcte du stockage. • Résoudre les échecs lors de la vérification du certificat SSL.
`La connexion a expiré`	L'adresse IP du serveur S3 est inaccessible	Vérifier la connectivité du réseau entre la grappe et le serveur S3
`Connexion à l'URL impossible`	Région du compartiment incorrecte	Saisissez la bonne région du compartiment
	URL non valide	Saisissez à nouveau l'URL correcte du point de terminaison de stockage S3
`Interdit`	Clé secrète non valide	Saisissez la clé secrète correcte du stockage
	Clé d'accès non valide	Saisissez la clé d'accès correcte du stockage
`Impossible de vérifier la configuration S3`	Autres exceptions ou erreurs génériques	Essayez de configurer le stockage S3 après un certain temps

Codes d'erreur des points de contrôle

Le tableau répertorie les codes d'erreur courants des points de contrôle et ne constitue pas une liste exhaustive.

Table 43: Codes d'erreur des points de contrôle

Code d'erreur	Description
E101 : Échec du point de contrôle de la base de données	Impossible de prendre un instantané des journaux des opérations de Mongodb
E102 : Échec du point de contrôle des données de flux	Impossible de prendre un instantané de la base de données Druid
E103 : Échec du chargement de l'instantané de base de données	Impossible de télécharger l'instantané de la base de données Mongo
E201 : Échec de copie de base de données	Impossible de charger l'instantané Mongo dans HDFS
E202 : Échec de copie de configuration	Impossible de télécharger l'instantané de consultation ou coffre-fort dans HDFS
E203 : Échec du point de contrôle de la configuration	Impossible de vérifier les données de consultation ou coffre-fort
E204 : Incompatibilité des données de configuration au point de contrôle	Impossible de générer un point de contrôle de consultation ou de coffre-fort après le nombre maximal de tentatives
E301 : Échec du téléchargement des données de sauvegarde	Échec du point de contrôle HDFS
E302 : Échec de téléchargement du point de contrôle	Le pilote de copie n'a pas réussi à charger les données dans S3
E401 : Mise à niveau du système au point de contrôle	La grappe a été mise à niveau à ce point de contrôle; le point de contrôle ne peut pas être utilisé
E402 : Redémarrage du service au point de contrôle	BkpDriver a redémarré à l'état de création; le point de contrôle ne peut pas être utilisé
E403 : Échec au point de contrôle précédent	Échec du point de contrôle lors de l'exécution précédente
E404 : Un autre point de contrôle en cours	Un autre point de contrôle est en cours
E405 : Impossible de créer le point de contrôle	Erreur dans le sous-processus de point de contrôle
Échec : terminé	Un point de contrôle précédent a échoué; il s'agit probablement d'un chevauchement de plusieurs points de contrôle démarrant en même temps.

Erreurs lors du processus de restauration des données

- Phase de configuration du stockage : pour obtenir des suggestions de résolution des problèmes lors de la configuration du stockage S3, consultez la section *Scénarios d'erreur des vérifications de la configuration S3*.
- Vérifications préalables pour vérifier l'intégrité de la grappe secondaire : pour les services qui ne sont pas intègres ou ceux qui ont des avertissements, accédez à la page Service Status (État du service) pour obtenir de plus amples renseignements afin d'assurer l'intégrité des services.
- Vérifications préalables pour vérifier la connectivité au stockage :

Table 44: Erreurs lors des vérification préalables de la connectivité de stockage

Scénario d'erreur	Description
Impossible de télécharger les données à partir du stockage S3 configuré.	En raison de la connectivité du réseau, l'accès au stockage S3 a échoué. Le message d'erreur persiste jusqu'à ce qu'un nouveau point de contrôle soit extrait du stockage S3 après le rétablissement de la connectivité.
L'UGS de grappe secondaire (de secours) est incompatible avec la grappe principale.	Assurez-vous de restaurer les données d'une grappe 39 RU vers une autre grappe 39 RU uniquement. De même, les données de la grappe 8 RU ne peuvent être restaurées que dans une grappe 8 RU.
La version de la grappe secondaire (de secours) est différente de la grappe principale.	Assurez-vous que les grappes principale et secondaire exécutent la même version.
Échec de la restauration de la base de données MongoDB	Impossible de restaurer les métadonnées de MongoDB. Le problème sera résolu lors de la prochaine prélecture de point de contrôle.
Le document DBRInfo est dans un format inconnu.	Les métadonnées du point de contrôle dans le stockage S3 sont endommagées ou le document se trouve dans un stockage incorrect. Téléchargez le fichier *dbrinfo.json* à partir du stockage S3 et partagez-le avec le centre d'assistance technique Cisco TAC pour vérification.
Synchronisation impossible avec le service de copie.	Erreurs internes entre le gestionnaire de restauration des données et le service de copie S3. Communiquez avec le centre d'assistance technique (Cisco TAC) pour résoudre le problème.

- Vérifications préalables du nom de domaine complet (FQDN) : si un panneau d'avertissement s'affiche à côté des vérification préalables du nom de domaine complet (FQDN), cela signifie que l'entrée DNS pour les noms de domaine complets ne pointe pas vers la grappe secondaire.

  Résolution : après la restauration des données, modifiez l'entrée DNS pour activer la connectivité entre les agents logiciels et la grappe secondaire.

- Phase de restauration des données : dans la boîte de dialogue de confirmation de la restauration des données, si la case de l'orchestrateur externe n'est pas une coche verte, vérifiez la connectivité entre la grappe secondaire et les orchestrateurs externes.

Note Une fois les données restaurées et que la grappe secondaire a atteint l'état principal, la page de restauration des données est toujours accessible pour vérifier le temps qui a été nécessaire et le nombre d'agents qui se sont reconnectés. Pour une grappe où les données ne sont jamais restaurées, la page de restauration des données est vide.

Haute disponibilité dans Cisco Secure Workload

Cisco Secure Workload offre une haute disponibilité en cas de probabilité de défaillance des services, des nœuds et des machines virtuelles. La haute disponibilité fournit des méthodes de récupération en assurant un temps d'arrêt minimal et une intervention minimale de l'administrateur du site.

Dans Cisco Secure Workload, les services sont répartis sur les nœuds d'une grappe. Plusieurs instances de services sont exécutées simultanément sur les nœuds. Une instance principale et une ou plusieurs instances secondaires sont configurées pour une haute disponibilité sur plusieurs nœuds. Lorsque l'instance principale d'un service tombe en panne, une instance secondaire du service est considérée comme principale et devient active immédiatement.

Conception de grappe de Cisco Secure Workload

Les composants clés d'une grappe Cisco Secure Workload sont les suivants :

- Des serveurs sans système d'exploitation qui hébergent plusieurs machines virtuelles, qui hébergent à leur tour de nombreux services.
- Serveurs sur bâti Cisco UCS de série C avec les commutateurs de la gamme Cisco Nexus 9300 qui contribuent à un réseau intégré haute performance.
- Modèles d'appareils matériels en petit ou grand format pour prendre en charge un nombre précis de charges de travail :
  - Déploiement de petit format avec six serveurs et deux commutateurs Cisco Nexus 9300.
  - Déploiement de grand format avec 36 serveurs et trois commutateurs Cisco Nexus 9300.

Figure 435: Conception de la conception de grappe Cisco Secure Workload

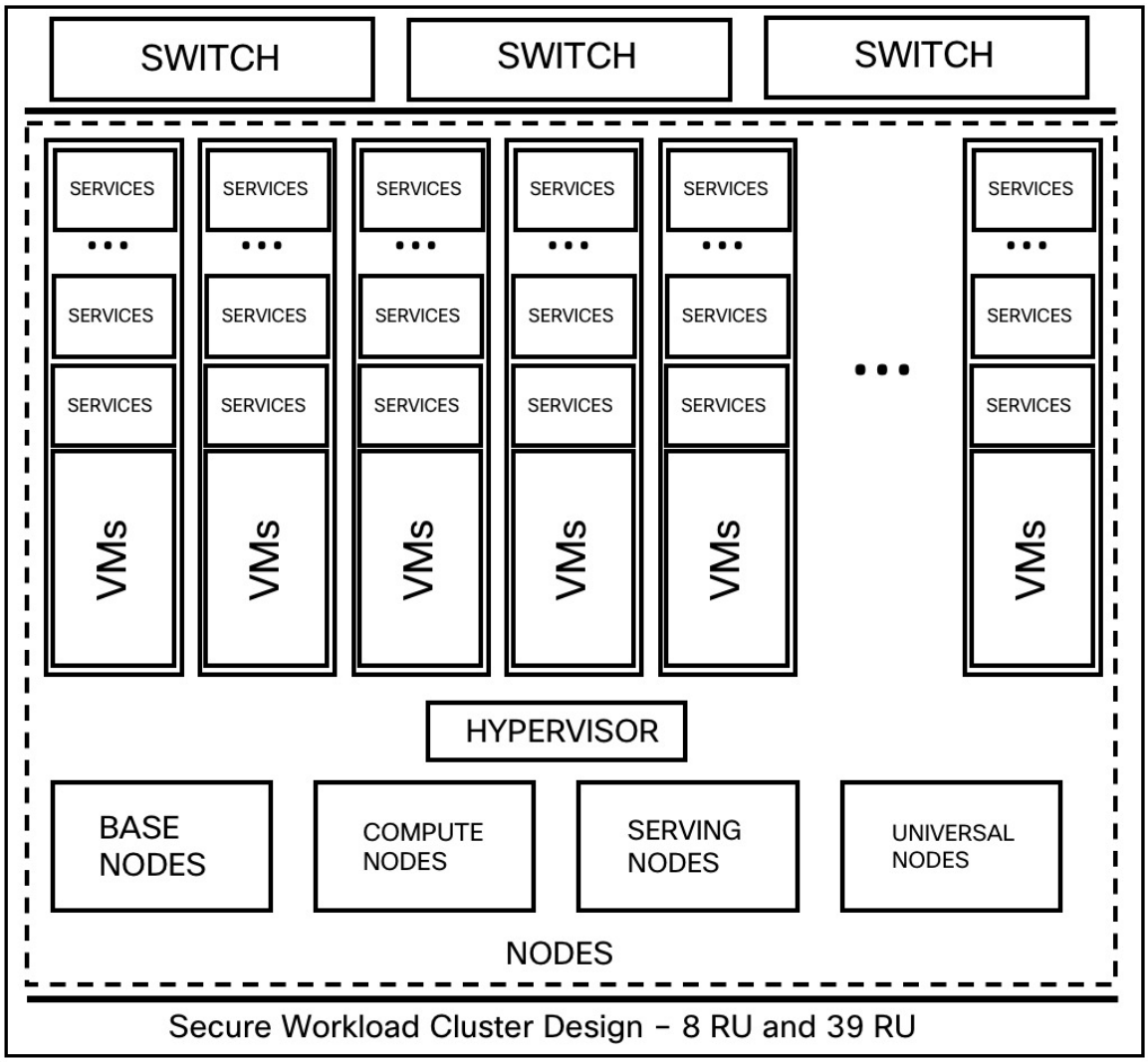


Table 45: Composants de la grappe Cisco Secure Workload

Attributs/Format	8 RU	39 RU
Nombre de nœuds	6	36
Nombre de nœuds de traitement informatiques	—	16
Nombre de nœuds de base	—	12
Nombre de nœuds de service	—	8
Nombre de nœuds universels	6	—
Nombre de machines virtuelles	50	106

Attributs/Format	8 RU	39 RU
Nombre de collecteurs	6	16
Nombre de commutateurs de réseau	2	3

Limites de la haute disponibilité dans Cisco Secure Workload

- Dans les deux formats (8RU et 39RU) de grappe, si un nœud défaillant héberge une machine virtuelle NameNode Hadoop, une intervention manuelle est nécessaire pour basculer vers une machine virtuelle NameNode secondaire.

Note Le basculement n'est pas automatique dans les versions 3.8.x et antérieures de Cisco Secure Workload.

- À partir de la version 3.9.x de Cisco Secure Workload, dans les facteurs de forme de grappe 8RU et 39RU, si un nœud qui héberge une VM Hadoop NameNode est défaillant, il n'est pas nécessaire d'intervenir manuellement pour basculer vers une VM secondaire.
- Avant d'effectuer une MISE À NIVEAU ou un REDÉMARRAGE, une intervention manuelle est nécessaire si la vérification préalable à la mise à niveau indique que Namenode-1 n'est pas actif ou dans un état normal. Si tel est le cas, vous devez effectuer un `POST namenode_failover` sur `launcherHost-1.node.consul` (ou sur tout autre `launcherHosts` en cours d'exécution) à partir de la page Explore.

Note Le basculement n'est pas automatique dans les versions 3.8.x et antérieures de Cisco Secure Workload.

- Pour un service à 2 ou 3 VM, comme les orchestrateurs, Redis, MongoDB, Elasticsearch, enforcementpolicystore, AppServer, ZooKeeper, TSDB, Grafana etc., une seule défaillance de machine virtuelle est prise en charge; une deuxième défaillance de la machine virtuelle rend le service inactif.

Impact and Recovery Details for Failure Scenarios

In Secure Workload, services are distributed across the nodes in a cluster. Multiple instances of services run simultaneously across the nodes. A primary instance and one or more secondary instances are configured for high availability across multiple nodes. When the primary instance of a service fails, a secondary instance of the service renders as primary and becomes active immediately.

- There is no impact to the cluster operation at any point in time.
- There is no single point of failure. If any of the nodes or VMs within the cluster fail, it does not result in failure of the entire cluster.
- There is minimal downtime of recovery from failure due to services, nodes, or VMs.

- There is no impact on the connections that are maintained by software agents to the Secure Workload cluster. The agents communicate with all the available collectors in the cluster. If a collector or VM fails, the software agents' connections to the other instances of the collectors ensure that the flow of data is not interrupted and there is no loss of functionality.
- The cluster services communicate with external orchestrators. When the primary instance of that service fails, the secondary instances take over to ensure the communication with external orchestrators is not lost.

Types of Failure Scenarios

High availability supports the following failure scenarios:

- Services Failure
- VM Failure
- Node Failure
- Network Switch Failure

Services Failure

When one or more services fail on any of the nodes, another instance of that particular service picks up and continues to run.

Figure 436: Normal Operation

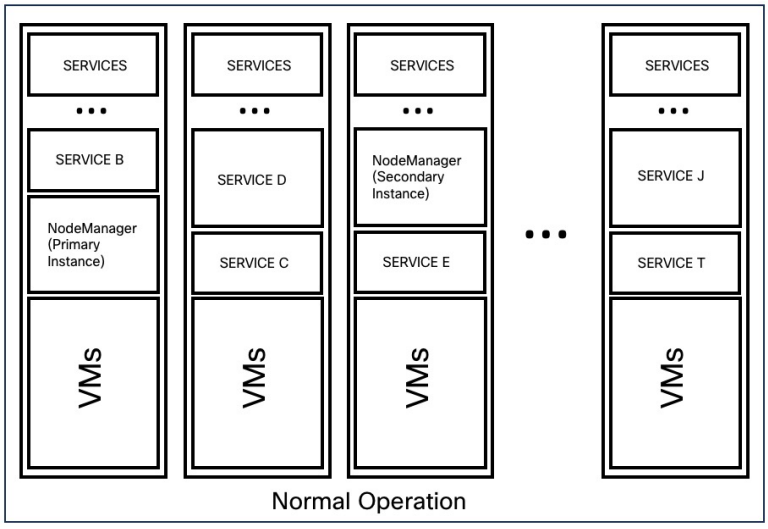
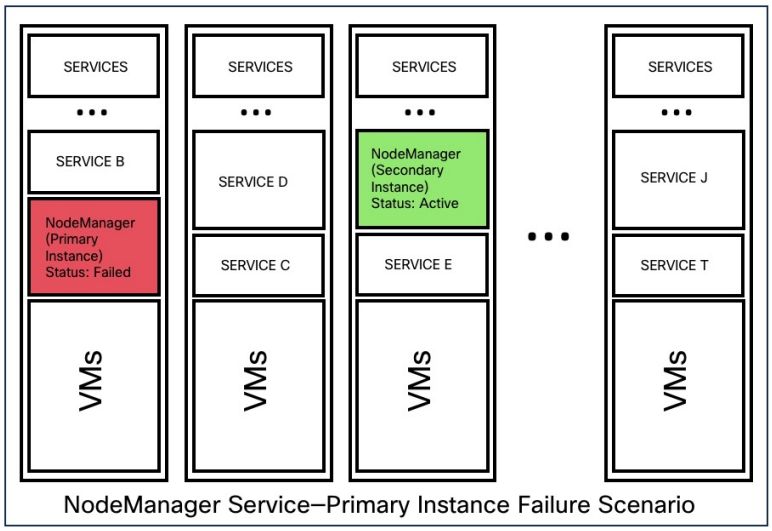


Figure 437: Failure Scenario of a Service



Impact	No visible impact.
Recovery	• Minimal downtime for the UI or dependent services to continue to run from the secondary instances. • Recovery is automatic.

VM Failure

When one of the VMs fails, the secondary VMs are available. The services on the secondary VMs pick up from where the services on the failed VM were running. Secure Workload restarts the failed VM to recover it. For example, as illustrated in the **Failure Scenario of a VM**, VM1 has failed and as a result the services running on it also has failed. The secondary VMs continue to be operational and the secondary instances picks up from where the services on the failed VM were running.

Figure 438: Normal Operation

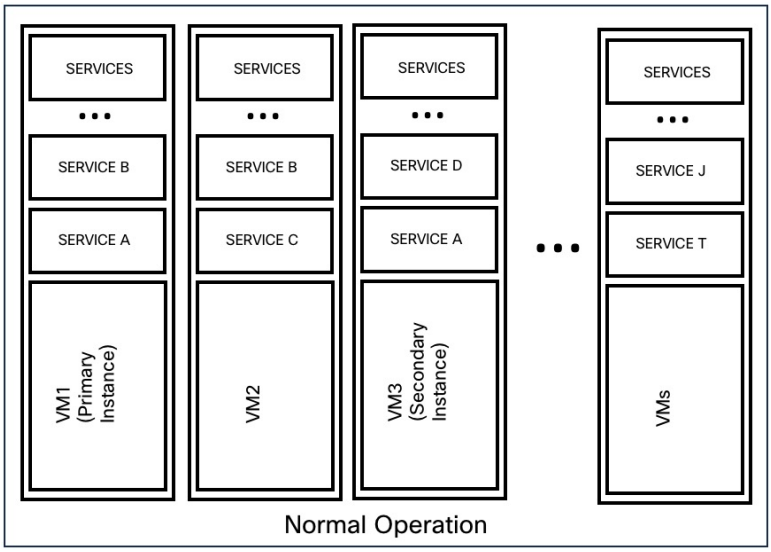
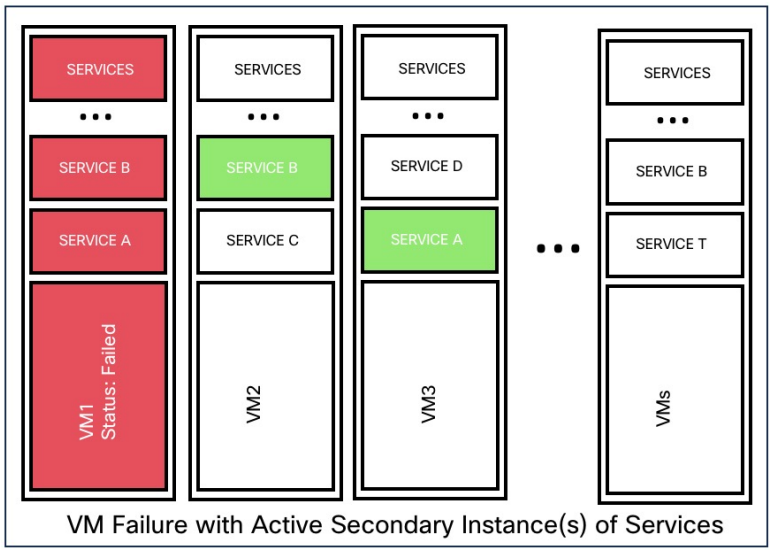


Figure 439: Failure Scenario of a VM



For services provided by symmetric VMs, such as collectordatamovers, datanode, nodemanager, and druidHistoricalBroker VMs, multiple VMs can fail but the applications will continue to function at reduced capacity.

Symmetric VM types:

Service Type	Total VMs	Number of VM Failures Supported
Datanode	6	4
DruidHistorical	4	2

Service Type	Total VMs	Number of VM Failures Supported
CollectorDataMover	6	5
NodeManager	6	4
UI/ AppServer	2	1

The nonsymmetric VM types tolerate only one VM failure before the services are rendered as unavailable.

Impact	No visible impact.
Recovery	• Minimal downtime for the UI or dependent services to continue to run from the secondary instances on other VMs. • Recovery is automatic. However, if a VM remains inactive for a longer duration, contact the TAC team to troubleshoot and find the RCA. You may need to replace the bare metal in a few instances.

Node Failure

Number of node failures tolerated:

Node Failures	8 RU	39 RU
Number of nodes that can fail for high availability	1	1*

* In 39 RU clusters, single node failure is always tolerated. A second node failure may be allowed as long as the two failed nodes do not host VMs for a 2 or 3-VM service, such as orchestrators, redis, mongodb, elasticsearch, enforcementpolicystore, appServer, zookeeper, TSDB, Grafana, and so on. In general, the second node failure results in a critical service becoming unavailable due to two VMs being affected. We recommend that you immediately restore the node upon a single node failure as the failure of a second node will most likely result in an outage.

Figure 440: Normal Operation

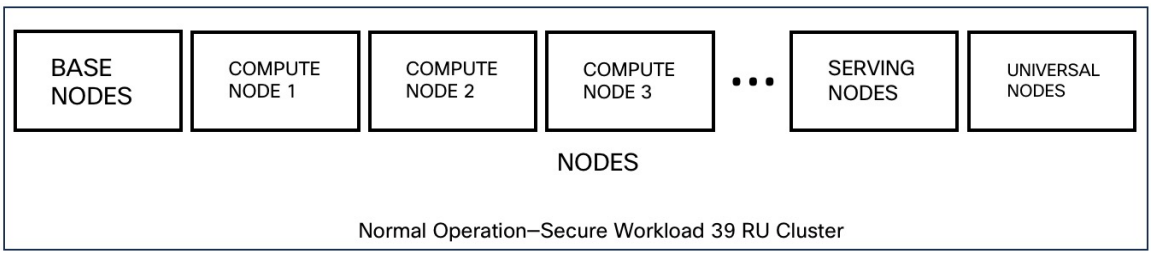
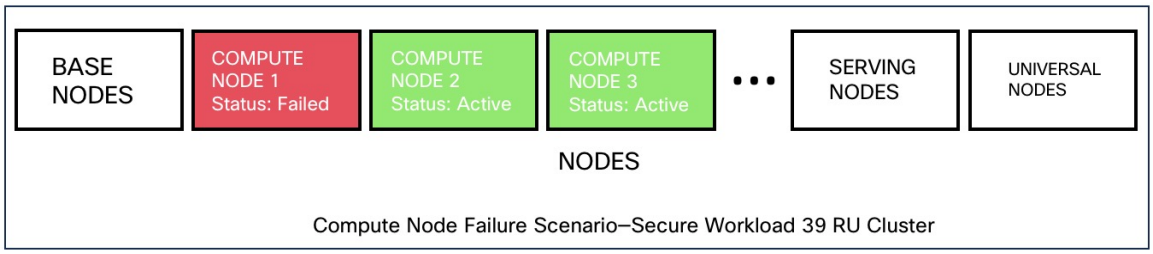


Figure 441: Failure Scenario of a Node



Impact	No impact in the functionality of the cluster. However, replace the failed node immediately using the RMA process. Failure of a second node will most likely result in an outage.
Recovery	• Minimal downtime. • If a node fails, we recommend that you contact Cisco TAC for assistance to remove the faulty node and replace it with another node.

Network Switch Failure

The switches in Secure Workload always remain active. In the 8 RU form factor deployment, there is no impact if a switch fails. In the 39 RU for factor deployment, the clusters experience half the input capacity if a switch fails. The switches do not have the recommended port density to support the VPC configuration for public networks.

Figure 442: Normal Operation

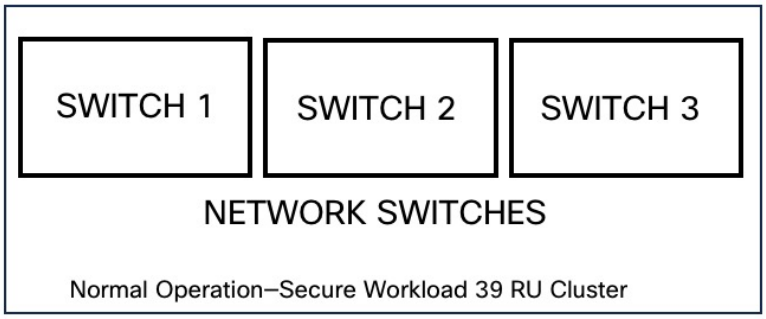
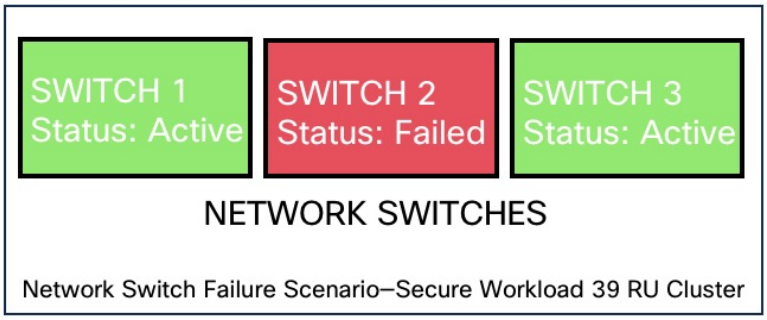


Figure 443: Failure Scenario of a Switch



Number of switch failures tolerated:

Form Factor	**8 RU**	**39 RU**
Number of switches that can fail for high availability	1 If two or more switches fail, it is likely to have an impact on the entire functionality of the cluster.	1* * A single switch failure results in half input capacity, two or more failures will likely impact the entire functionality of the cluster.

Impact	• A faulty switch or network card on a bare metal causes loss of network connectivity within the cluster. • No impact in the functionality of the cluster because of a single switch failure. However, two or more failures will likely impact the entire functionality of the cluster. • Connectivity issues to multiple VMs on the cluster, or intermittent and prolonged connectivity problems result in unpredictable behaviour within the cluster.
Recovery	• Recovery is automatic. • Contact Cisco TAC for assistance in troubleshooting faulty switches or network cards on bare metals.

Renseignements sur la machine virtuelle

La page **Virtual Machine** (Machines virtuelles), sous le menu **Troubleshoot** (Dépannage), affiche toutes les machines virtuelles qui font partie de la grappe Cisco Cisco Secure Workload. Elle affiche leur état de déploiement pendant le démarrage ou la mise à niveau (le cas échéant), ainsi que les adresses IP publiques.

Notez que toutes les machines virtuelles de la grappe ne font pas partie d'un réseau public, par conséquent, elles peuvent ne pas avoir d'adresse IP publique.

Mise à niveau d'une grappe Cisco Secure Workload

Cisco Secure Workload prend en charge deux types de mise à niveau : la mise à niveau complète et la mise à niveau avec correctifs. Les sections suivantes décrivent le processus de mise à niveau complète. Pendant la mise à niveau complète, toutes les machines virtuelles de la grappe sont arrêtées, de nouvelles machines virtuelles sont déployées et les services sont mis en service à nouveau. Toutes les données de la grappe sont conservées pendant cette mise à niveau, à l'exception du temps d'arrêt pendant la mise à niveau.

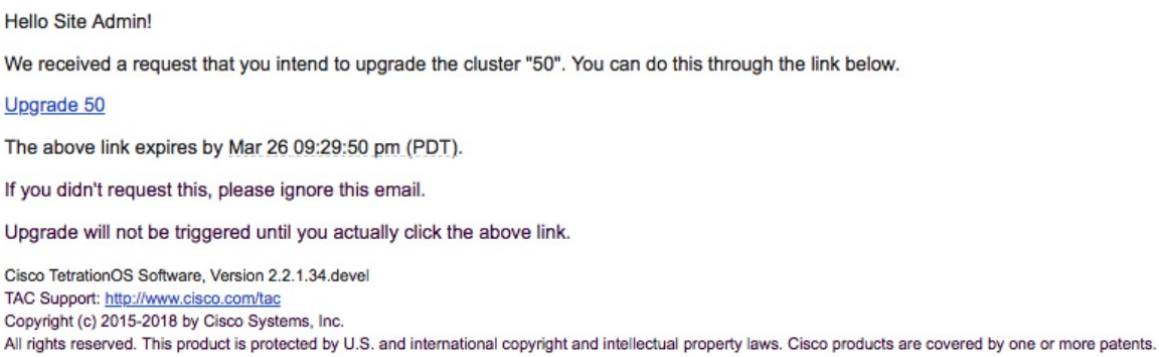
Options de mise à niveau de grappe

Types de mise à niveau prises en charge pour une grappe Cisco Secure Workload :

- **Mise à niveau complète** : pour lancer la mise à niveau complète, dans le volet de navigation, choisissez **Platform(Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**. Dans l'onglet **Upgrade** (Mettre à niveau) , select **Upgrade** (Mettre à niveau). Pendant le processus de mise à niveau complet, les machines virtuelles sont éteintes, et sont mises à niveau et redéployées. Il se produit un temps d'arrêt de la grappe pendant lequel l'interface utilisateur de Cisco Secure Workload est inaccessible.
- **Mise à niveau des correctifs** : La mise à niveau des correctifs réduit le temps d'arrêt de la grappe. Les services auxquels un correctif doit être appliqué sont mis à jour et n'entraînent pas le redémarrage de la machine virtuelle. Le temps d'arrêt est généralement de l'ordre de quelques minutes. Pour lancer la mise à niveau des correctifs, sélectionnez **Patch Upgrade** (Mise à niveau de correctifs) et cliquez sur **Send Patch Upgrade Link** (Envoyer le lien de mise à niveau des correctifs).

Un courriel contenant un lien est envoyé à l'adresse courriel enregistrée pour lancer la mise à niveau.

Figure 444: Courriel contenant le lien de mise à niveau


Hello Site Admin!

We received a request that you intend to upgrade the cluster "50". You can do this through the link below.

Upgrade 50

The above link expires by Mar 26 09:29:50 pm (PDT).

If you didn't request this, please ignore this email.

Upgrade will not be triggered until you actually click the above link.

Cisco TetrationOS Software, Version 2.2.1.34.devel
TAC Support: http://www.cisco.com/tac
Copyright (c) 2015-2018 by Cisco Systems, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Cisco products are covered by one or more patents.

Avant d'envoyer le courriel, l'orchestrateur exécute plusieurs vérifications pour s'assurer que la grappe peut être mise à niveau. Les vérifications comprennent les actions suivantes :

- Vérifie qu'il n'y a aucun nœud mis hors service.
- Vérifie chaque élément nu pour s'assurer qu'il n'y a aucune défaillance matérielle, notamment des éléments suivants :
    - Défaillance du lecteur

- Défaillance prédictive du lecteur.
- Lecteur manquant
- Échecs de StorCLI
- Échecs des journaux MCE

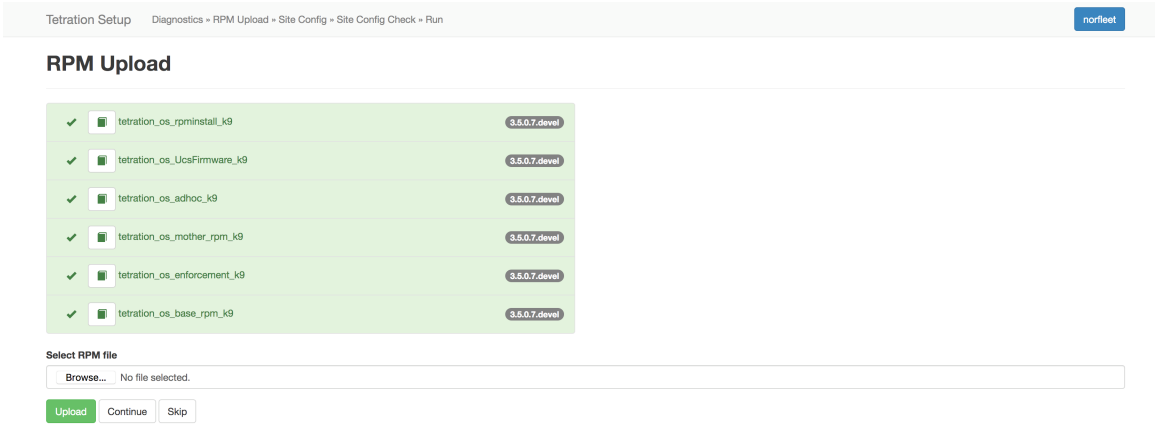
- Effectue des vérifications pour s'assurer que les machines à l'état sans système d'exploitation sont en service, qu(il n'y a pas moins de 36 serveurs pour le 39RU et six pour le 8RU.

Note En cas de défaillance, un lien de mise à niveau n'est pas envoyé à l'adresse courriel enregistrée et une erreur 500 s'affiche avec des informations telles qu'une défaillance matérielle ou un hôte manquant. Vérifiez les journaux de l'orchestrateur pour plus d'informations. Dans ce scénario, utilisez explore jusqu'à -100 sur /local/logs/tetration/orchestrator/orchestrator.log dans le fichier hôte orchestrator.service.consul. Le journal fournit des renseignements détaillés pour déterminer laquelle des trois vérifications est à l'origine de l'échec. Cela nécessite généralement de réparer le matériel et de remettre le nœud en service. Redémarrer le processus de mise à niveau.

RPM Upload

Click on the link in the email will connect to the setup UI in the cluster. Setup UI is a operations UI that will be used for deploy/upgrade of the cluster. The initial page will show the list of RPMs that are currently installed in the cluster. This is also the upload page to upload all the RPMs

Figure 445: RPM Upload



Upload the RPMs in the order that is shown on setup UI. The order is

1. tetration_os_rpminstall_k9
2. tetration_os_UcsFirmware_k9
3. tetration_os_adhoc_k9
4. tetration_os_mother_rpm_k9

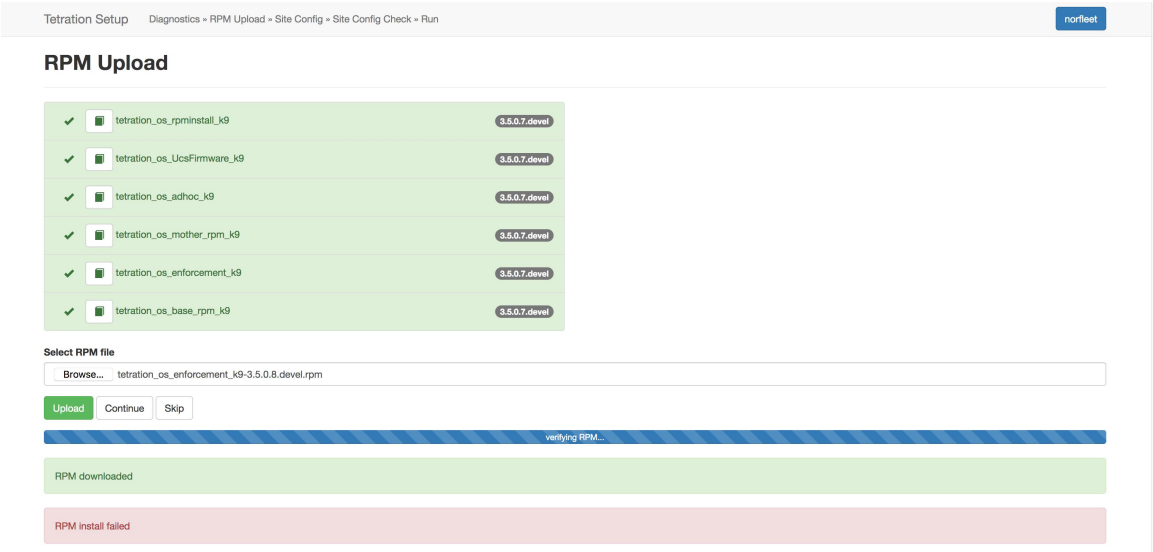
5. tetration_os_enforcement_k9
6. tetration_os_base_rpm_k9

Note For Cisco Secure Workload Virtual clusters deployed on vSphere, please be sure to also upgrade the tetration_os_ova_k9 RPM and do not upload the tetration_os_base_rpm_k9.

Uploading any other order will result in upload failure. Until all the RPMs are uploaded in the correct order Continue button will be disabled.

Logs for each upload can be seen by clicking on the Log symbol on the left of every RPM. Also uploads that failed will be marked RED in color.

Figure 446: RPM Upload log



Informations sur le site

L'étape suivante de la mise à niveau de la grappe consiste à mettre à jour les renseignements du site. Tous les champs de renseignements du site ne peuvent pas être mis à jour. Seuls les champs suivants peuvent être mis à jour :

- Clé publique SSH
- Courriel d'alerte Sentinel (pour Boosun)
- Réseau interne du contrôleur CIMC
- Passerelle de réseau interne du contrôleur CIMC
- Réseau externe

Note Ne modifiez pas le réseau externe existant. Vous pouvez ajouter des réseaux supplémentaires en les ajoutant à ceux existants. La modification ou la suppression du réseau existant rendra la grappe inexploitable.

- résolveurs DNS
- Domaines DNS
- Serveurs NTP
- SMTP Server
- Port SMTP
- Nom d'utilisateur SMTP (facultatif)
- Mot de passe SMTP (facultatif)
- Serveur Syslog (facultatif)
- Port Syslog (facultatif)
- Niveau de gravité Syslog (facultatif)

Note

- La gravité du serveur syslog varie de critique à informatif. La gravité doit être réglée à « avertissement » ou à un niveau supérieur (à titre indicatif) pour les alertes.
- À partir de la version 3.1, **le journal système externe via l'interface utilisateur de configuration n'est pas pris en charge**. Configurez l'appareil TAN pour exporter les données vers SYSLOG. Pour de plus amples renseignements, consultez la section La tunnellisation Syslog externe est transférée vers le TAN.
- Cisco Secure Workload prend en charge la communication sécurisée SMTP vers les serveurs de messagerie qui prennent en charge la communication SSL ou TLS à l'aide de la commande STARTTLS. Le port standard des serveurs qui prennent en charge le trafic sécurisé est généralement le port 587/TCP, mais de nombreux serveurs acceptent également les communications sécurisées sur le port standard 25/TCP.

  Cisco Secure Workload ne prend pas en charge le protocole SMTPS pour la communication avec les serveurs de messagerie externes.

Les autres champs ne peuvent pas être mis à jour. S'il n'y a aucun changement, cliquez sur **Continue** (Continuer) pour déclencher les vérifications préalables à la mise à niveau, sinon mettez les champs à jour, puis cliquez sur **Continue**.

Vérifications préalables à la mise à niveau

Avant de mettre à niveau la grappe, quelques vérifications sont effectuées sur celle-ci afin de s'assurer que tout est en ordre. Les vérifications préalables à la mise à niveau suivantes sont effectuées :

- Vérifications dans la version du RPM : vérifie pour s'assurer que tous les RPM sont téléversés et que la version est correcte. La vérification ne porte pas sur l'exactitude de la commande, mais sur le fait que la

version a été téléversée. Notez que les vérifications de la commande sont effectuées lors du chargement lui-même.

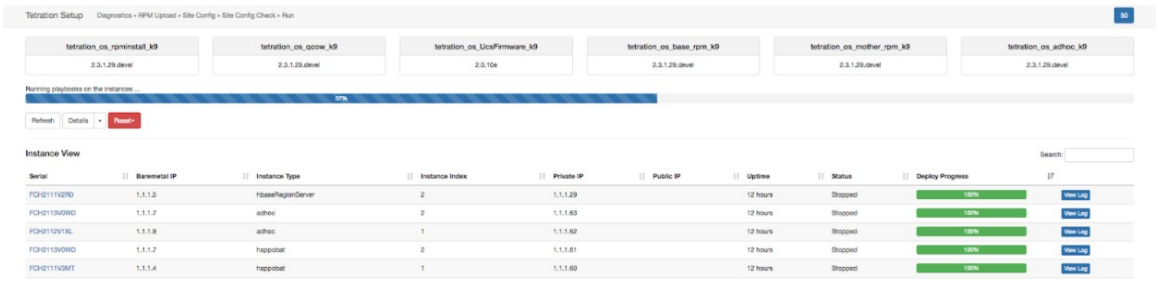
- Site Linter : effectue le linting des informations du site
- Configuration du commutateur : configure les commutateurs Leaves ou Spine
- Vérificateur de site : effectue les vérifications des serveurs DNS, NTP et SMTP. Envoie un courriel avec un jeton. Le courriel est envoyé au compte d'administrateur principal du site. Si l'un des services DNS, NTP ou SMTP n'est pas configuré, cette étape échoue.
- Validation du jeton : saisissez le jeton envoyé dans le courriel et continuez le processus de mise à niveau.

Mettre à niveau la grappe Cisco Secure Workload

Caution

- Nous vous recommandons de ne pas sélectionner l'option **Ignore stop Failures** (Ignorer les échecs d'arrêt). Il s'agit d'une option de récupération en cas d'échec de la mise à niveau lorsque certains services ne se ferment pas correctement. L'utilisation de cette option arrête les machines virtuelles qui peuvent créer des défaillances lorsque les services deviennent actifs.
- Utilisez cette option sous surveillance.

Figure 447: Mise à niveau de la grappe



Before you begin

Effectuez les vérifications préalables à la mise à niveau et saisissez le jeton reçu dans le *courriel de vérification du jeton*.

Procedure

Étape 1 Cliquez sur **Continue** (Continuer) pour commencer la mise à niveau.

Étape 2 (Facultatif) Cliquez sur le nom de la grappe pour afficher les renseignements sur le site.

Les RPM et les versions de Cisco Secure Workload sont affichés. La barre de mise à niveau affiche la progression de cette dernière. Le bleu indique les activités en cours, le vert les activités terminées et le rouge les activités qui ont échoué.

Quatre boutons sont disponibles :

- Refresh (Actualiser) : actualise la page.
- Details (Détails) : Cliquez sur **Details** (Détails) pour afficher les étapes qui ont été effectuées au cours de cette mise à niveau. Cliquez sur la flèche à côté du bouton pour afficher les journaux.
- Reset (Réinitialiser) : il s'agit d'une option pour réinitialiser l'état de l'orchestrateur. Cette option annule la mise à niveau et vous ramène au début. NE PAS L'UTILISER sauf si la mise à niveau a échoué et que quelques minutes se sont écoulées après l'échec de la mise à niveau pour que tous les processus soient terminés avant de redémarrer cette dernière.
- Restart (Redémarrer) : lorsqu'une mise à niveau échoue, cliquez sur **Restart** (Redémarrer) pour redémarrer la grappe et lancer une nouvelle mise à niveau. Cela peut permettre de résoudre les opérations de nettoyage en attente ou les problèmes qui bloquent les processus de mise à niveau.

Dans la vue de l'instance, chaque état de déploiement de machine virtuelle est suivi. Les colonnes comprennent :

- Série : série sans système d'exploitation qui héberge cette machine virtuelle
- IP sans système d'exploitation : l'adresse IP interne attribuée au routeur sans système d'exploitation
- Instance Type : le type de la machine virtuelle
- Index d'instance : index de la machine virtuelle : il existe plusieurs machines virtuelles du même type pour une haute disponibilité.
- Adresse IP privée : l'adresse IP interne attribuée à cette machine virtuelle
- Adresse IP publique : l'adresse IP routable attribuée à cette machine virtuelle. Toutes les machines virtuelles n'en ont pas.
- Disponibilité : temps de disponibilité de la machine virtuelle
- État : peut être Stopped, Deployed, Failed, Not Started ou In Progress (Arrêté, Déployé, Échec, Non démarré ou En cours).
- Avancement du déploiement : pourcentage de déploiement
- View Log (Afficher le journal) : bouton pour afficher l'état de déploiement de la machine virtuelle

Journaux de mise à niveau de grappe

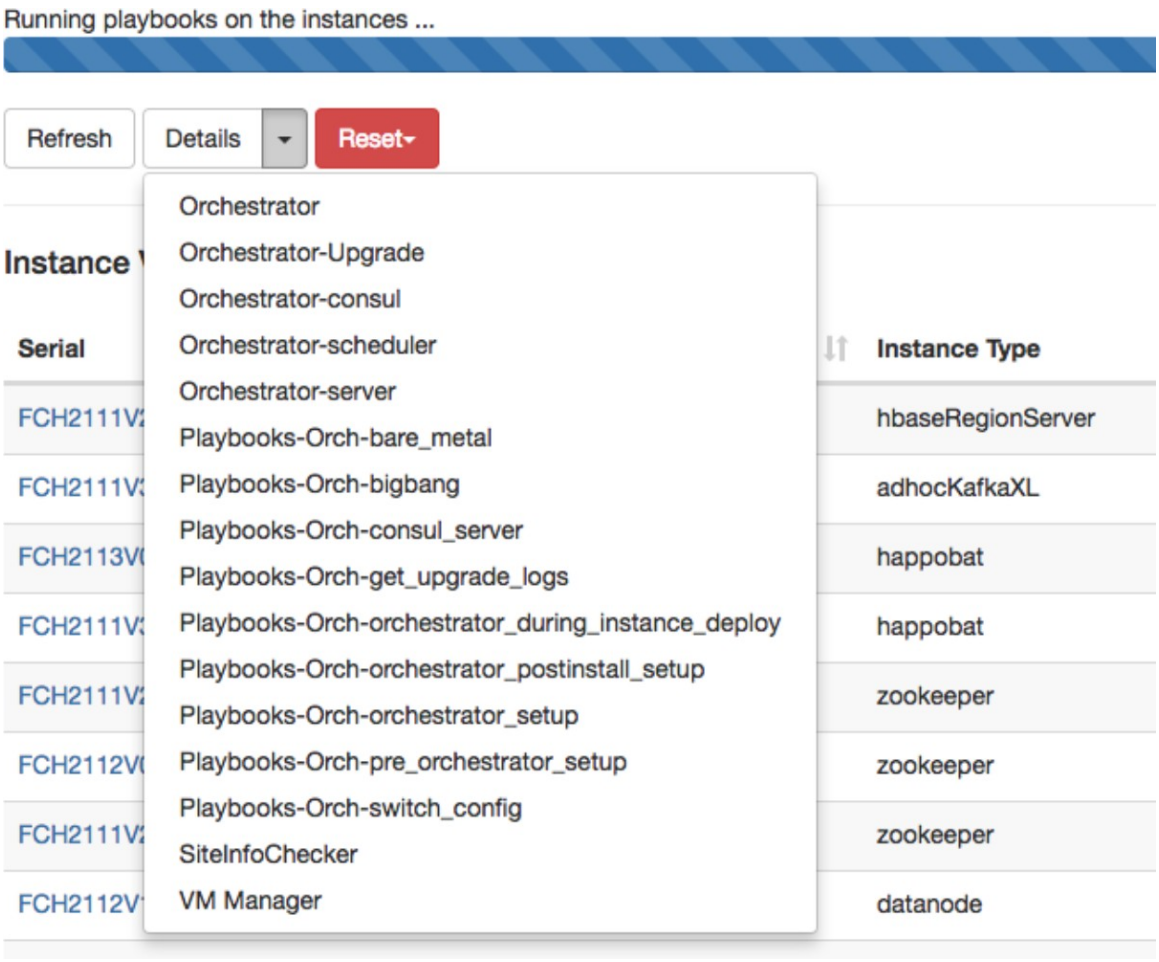
Il existe deux types de journaux :

Procedure

Étape 1 Journaux de déploiement de **machines virtuelles** : cliquez sur **View Log** (Afficher le journal) pour afficher les journaux de déploiement des machines virtuelles.

Étape 2 **Journaux d'orchestration** : Cliquez sur la flèche à côté du bouton **Details** (détails) pour afficher les journaux d'orchestration.

Figure 448: Journaux d'orchestration



Chacun des liens pointe vers les journaux.

- Orchestrateur - Journal de l'orchestrateur - c'est le premier endroit pour suivre la progression. Toute défaillance pointe vers un journal à consulter.
- Mise à niveau d'Orchestrator – non présente dans la version 2.3
- Orchestrator-consul – Journaux de conseil qui s'exécutent sur l'orchestrateur principal.
- Orchestrateur-Planificateur – Journaux du planificateur de machine virtuelle – quelle machine virtuelle a été placée sur quelle machine sans système d'exploitation et le journal de planification.
- Orchestrator-server – Journaux du serveur HTTP de l'orchestrateur.
- Playbooks-* : tous les journaux de guides qui s'exécutent sur l'orchestrateur.

Exécuter des vérifications avant la mise à niveau

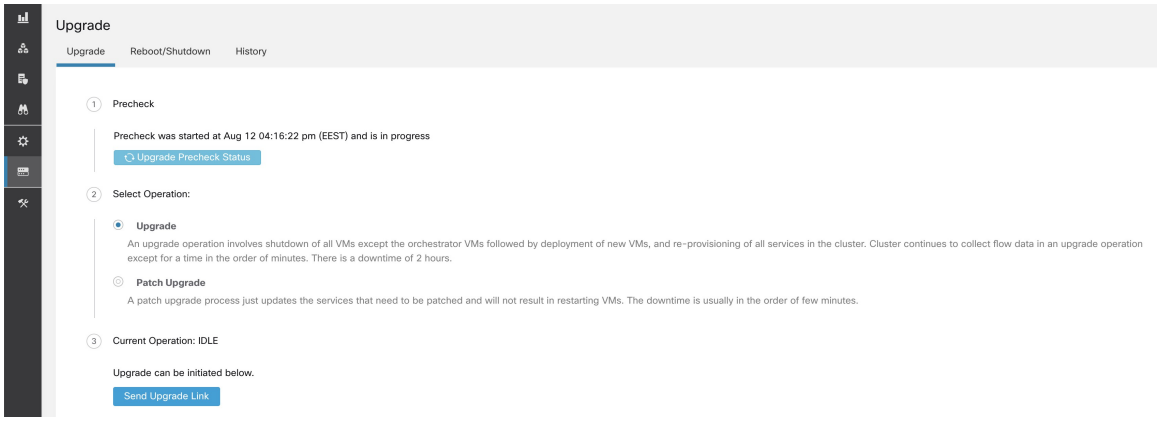
Il peut arriver que des défaillances matérielles se produisent ou que la grappe ne soit pas prête à être mise à niveau après la programmation et le lancement de cette dernière. Ces erreurs doivent être corrigées avant de procéder aux mises à niveau. Au lieu d'attendre une fenêtre de mise à niveau, vous pouvez lancer des vérifications préalables à la mise à niveau, qui peuvent être exécutées autant de fois que vous le souhaitez et à tout moment, sauf lors d'une mise à niveau, d'une mise à jour de correctifs ou d'un redémarrage.

Pour exécuter des vérifications avant la mise à niveau :

1. Dans l'onglet **Upgrade** (Mise à niveau), cliquez sur **Start Upgrade Precheck**(démarrer la vérification préalable à la mise à niveau).

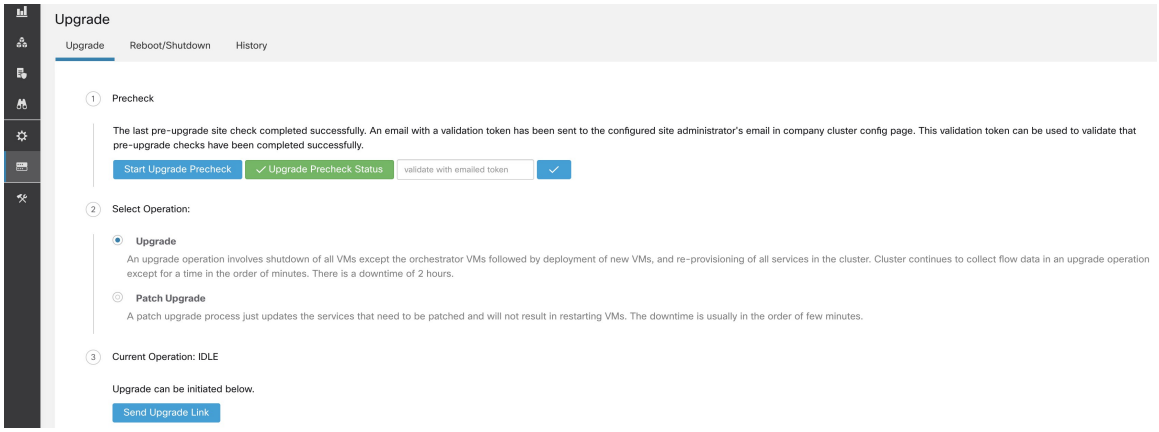
   Cela lance les vérifications préalables à la mise à niveau et passe l'état à En cours d'exécution.

   Figure 449: Exécution des vérifications préalables à la mise à niveau



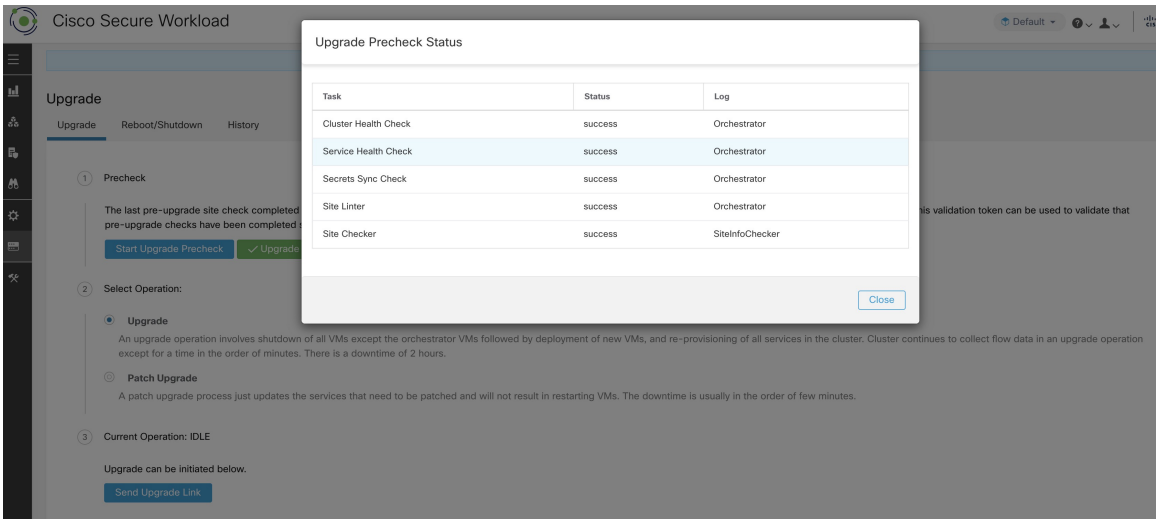
2. Une fois toutes les vérifications exécutées par les orchestrateurs réussies, un courriel avec un jeton est envoyé à l'ID de courriel enregistré. Saisissez le jeton pour terminer les vérifications préalables à la mise à niveau.

   Figure 450: Saisir un jeton pour les vérifications préalables à la mise à niveau



Vous pouvez vérifier l'état des vérifications. En cas d'échec des vérifications préalables à la mise à niveau, vous pouvez visualiser les vérifications qui ont échoué et le passage à l'état d'échec de la vérification concernée.

Figure 451: État des vérifications préalables à la mise à niveau



Sauvegarde et restauration des données (DBR)

Si **DBR** est activé sur la grappe, consultez également Mise à niveau avec la sauvegarde et la restauration des données

Instantanés de grappe Cisco Secure Workload

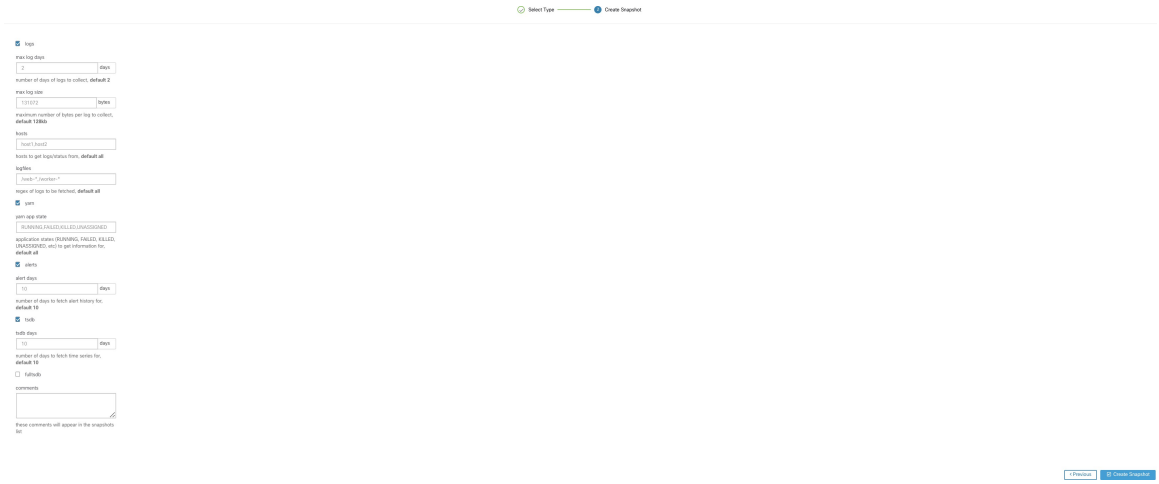
Accès à l'interface utilisateur de création d'instantanés

Les utilisateurs disposant du **rôle de service d'assistance à la clientèle** peuvent accéder à l'outil de capture d'instantanés en sélectionnant **Troubleshooting (Dépannage)** > **Snapshots(Instantanés)** dans la barre de navigation sur le côté gauche de la fenêtre.

Pour créer un instantané classique ou des offres groupées de support technique Cisco Integrated Management Controller (CIMC). Cliquer sur le bouton Create Snapshot (Créer un instantané) dans la page de la liste du fichier Instantané charge une page permettant de choisir un instantané classique ou CIMC (offre groupée de soutien technique). L'option permettant de choisir un instantané CIMC est désactivée sur les Cisco Secure Workload Logiciel uniquement (ESXi) et les logiciels-services Cisco Secure Workload.

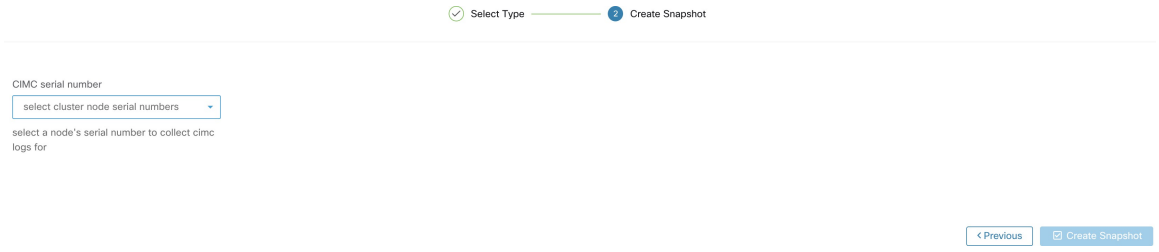
Cliquer sur le bouton d'instantané classique pour charger l'interface utilisateur du programme d'exécution de l'outil Snapshot (Instantané) :

Figure 452: Module d'exécution de l'outil Snapshot (Instantané)



Cliquer sur le bouton CIMC Snapshot (Instantané CIMC) pour charger l'interface utilisateur du programme d'exécution de l'outil de soutien technique de CIMC :

Figure 453: Programme d'exécution de l'outil de l'assistance technique CIMC



Créer un instantané

Sélectionnez **Create Snapshot** (Créer un instantané) avec les options par défaut, l'outil Snapshot recueille :

- Journaux
- L'état de l'application et des journaux Hadoop ou YARN
- L'historique des alertes
- De nombreuses statistiques de la TSDB

Il est possible de remplacer les valeurs par défaut et de préciser certaines options.

- Options du journal
  - max log days : nombre de jours de journaux à collecter, par défaut 2.
  - max log size : nombre maximal d'octets par journal à collecter, 128 Ko par défaut
  - hosts : hôtes pour obtenir les journaux/l'état, par défaut tous.
  - logfiles : expression régulière des journaux à récupérer, tous par défaut.

- options yarn
  - yarn app state ; États de l’application (RUNNING, FAILED, KILLED, UNASSIGNED, etc). pour obtenir des informations, par défaut tous.
- options d’alertes
  - alert days : le nombre de jours de données d’alerte à collecter.
- Options de tsdb
  - tsdb days : le nombre de jours de données tsdb à collecter. Son augmentation peut créer de très gros instantanés.
- Options Fulltsdb
  - fulltsdb : un objet JSON qui peut être utilisé pour spécifier startTime, endTime, FullDumpPath, localDumpFile et NameFilterInclureRegex pour limiter les mesures à collecter.
- comments : commentaires qui peuvent être ajoutés pour décrire la raison et l’entité qui recueille l’instantané.

Après avoir sélectionné Create Snapshot (Créer un instantané), une barre de progression pour l’instantané s’affiche en haut de la page de liste des fichiers d’instantané. Lorsque l’instantané est terminé, il peut être téléchargé à l’aide du bouton Download (Télécharger) sur la page de la liste des fichiers d’instantané. Un seul instantané peut être réalisé à la fois.

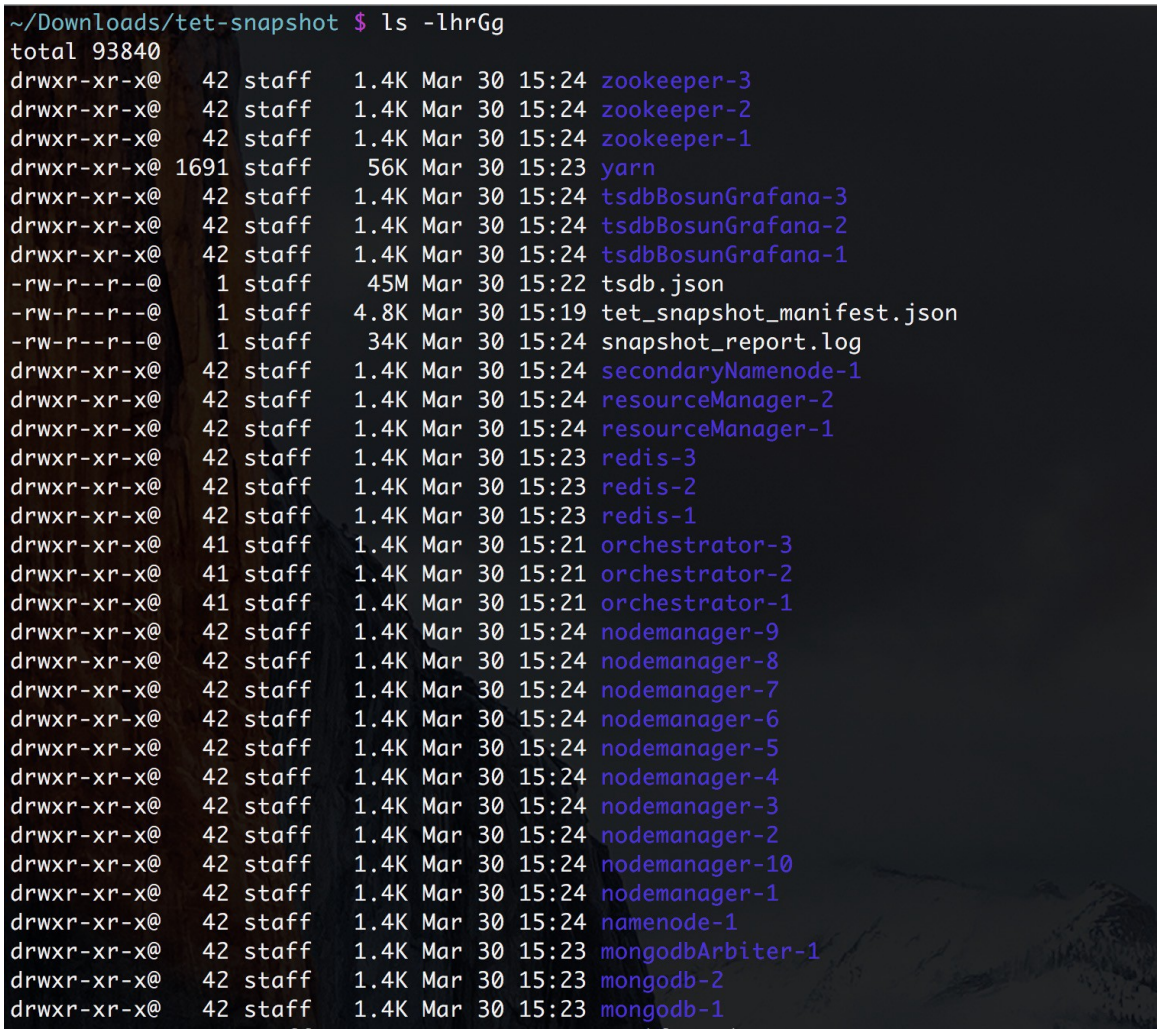
Création d'un ensemble de fichiers de soutien technique du CIMC

Sur la page CIMC Snapshot (Instantané CIMC) (ensemble de soutien technique), sélectionnez le numéro de série du nœud pour lequel l’ensemble de soutien technique CIMC doit être créé et cliquez sur le bouton **Create Snapshot** (Créer un instantané). Une barre de progression pour la collecte de l'ensemble de soutien technique du contrôleur CIMC s’affiche dans la page de liste des fichiers d’instantané et la section des commentaires indique que la collecte de l’ensemble de soutien technique du contrôleur CIMC a été déclenchée. Lorsque la collecte de l’ensemble de soutien technique du contrôleur CIMC est terminée, le fichier peut être téléchargé à partir de la page de liste des fichiers Snapshot Instantanés).

Utilisation d'un instantané

Le traitement d’un instantané crée un répertoire ./clustername_sNAPshot qui contient les journaux pour chaque machine. Les journaux sont enregistrés en tant que fichiers texte qui contiennent les données de plusieurs répertoires des machines. L’instantané enregistre également toutes les données Hadoop/TSDB enregistrées au format JSON.

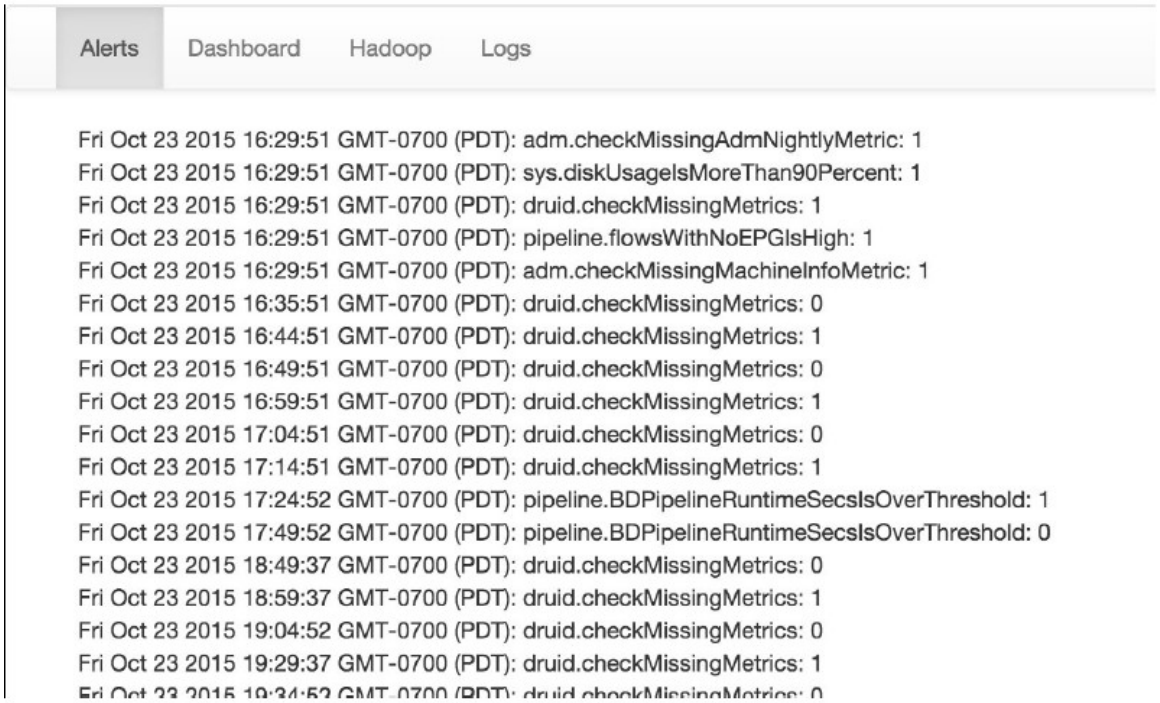
Figure 454: Utilisation d'un instantané



Lorsque vous ouvrez le fichier index.html dans un navigateur, vous trouverez des onglets concernant :

- Liste courte des changements d'état d'alerte.

Figure 455: Liste courte des changements d'état d'alerte

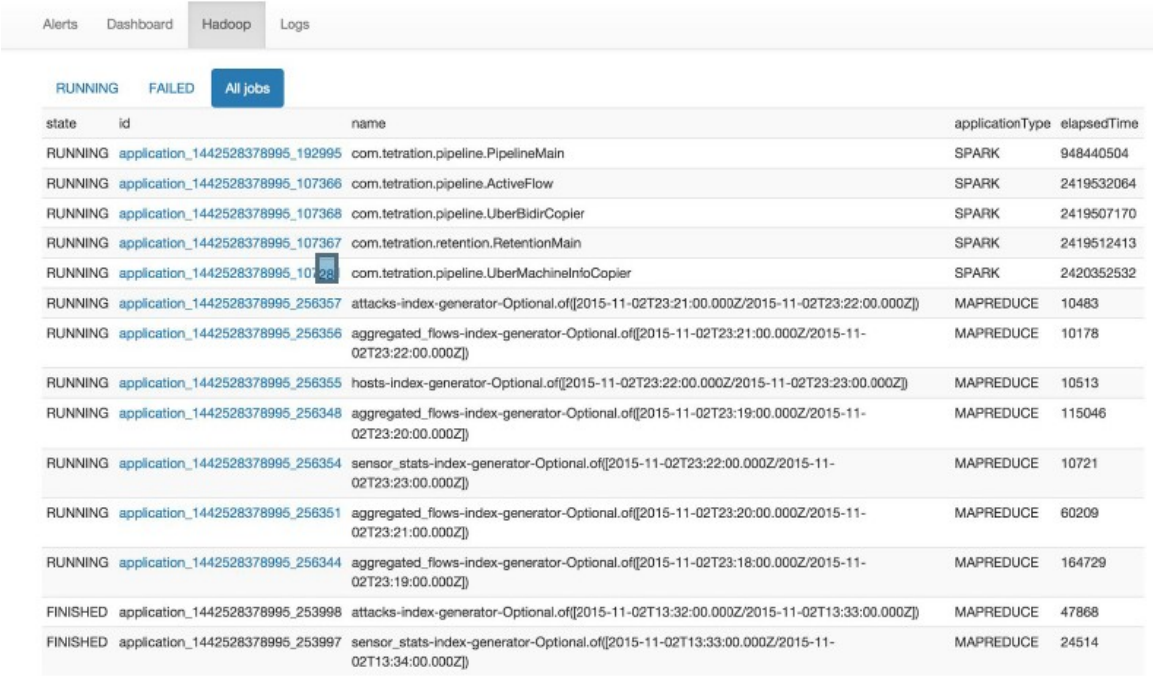


- Reproduction des tableaux de bord Graffana.

Figure 456: Reproduction des tableaux de bord Graffana

- Reproduction du serveur frontal Hadoop Resource Manager qui contient les tâches et leur état. La sélection d'une tâche affiche les journaux de la tâche.

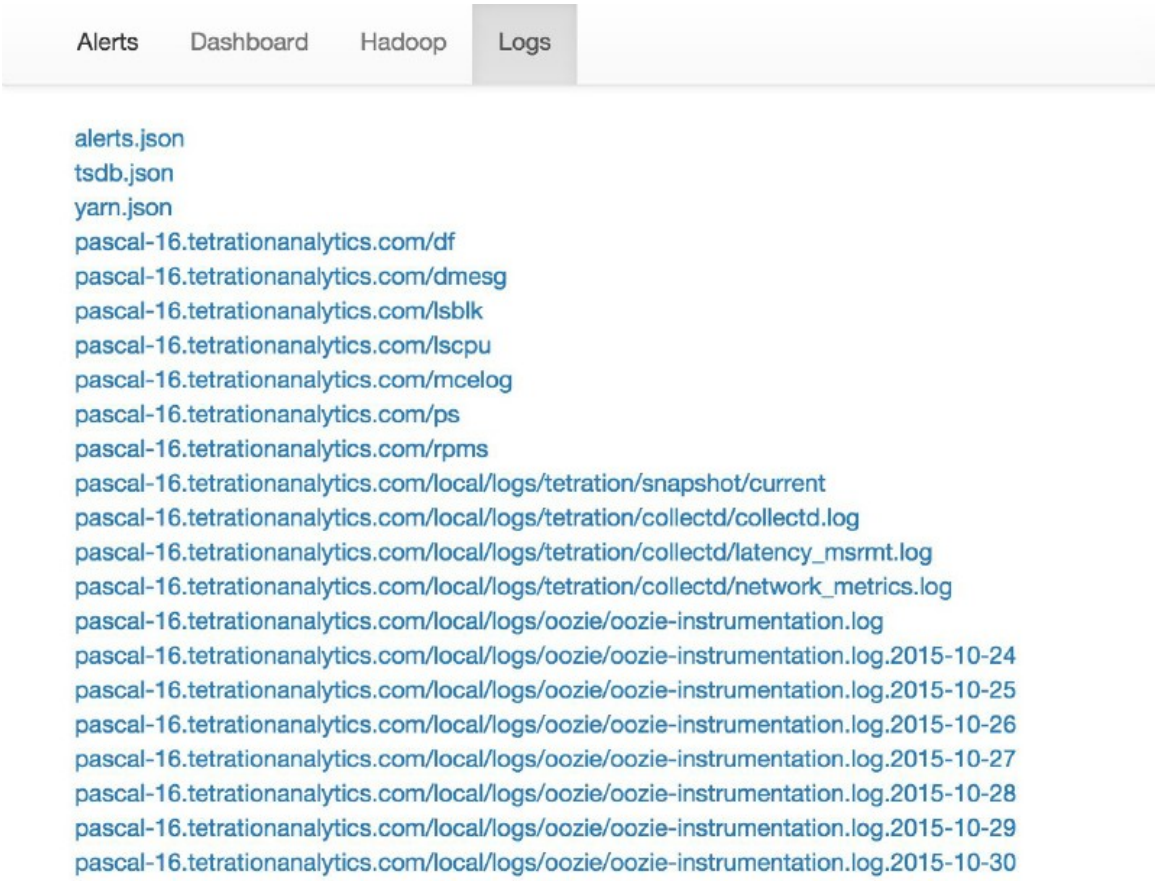
Figure 457: Reproduction du gestionnaire de ressources Hadoop



state	id	name	applicationType	elapsedTime
RUNNING	application_1442528378995_192995	com.tetration.pipeline.PipelineMain	SPARK	948440504
RUNNING	application_1442528378995_107366	com.tetration.pipeline.ActiveFlow	SPARK	2419532064
RUNNING	application_1442528378995_107368	com.tetration.pipeline.UberBidirCopier	SPARK	2419507170
RUNNING	application_1442528378995_107367	com.tetration.retention.RetentionMain	SPARK	2419512413
RUNNING	application_1442528378995_107281	com.tetration.pipeline.UberMachineInfoCopier	SPARK	2420352532
RUNNING	application_1442528378995_256357	attacks-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10483
RUNNING	application_1442528378995_256356	aggregated_flows-index-generator-Optional.of([2015-11-02T23:21:00.000Z/2015-11-02T23:22:00.000Z])	MAPREDUCE	10178
RUNNING	application_1442528378995_256355	hosts-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10513
RUNNING	application_1442528378995_256348	aggregated_flows-index-generator-Optional.of([2015-11-02T23:19:00.000Z/2015-11-02T23:20:00.000Z])	MAPREDUCE	115046
RUNNING	application_1442528378995_256354	sensor_stats-index-generator-Optional.of([2015-11-02T23:22:00.000Z/2015-11-02T23:23:00.000Z])	MAPREDUCE	10721
RUNNING	application_1442528378995_256351	aggregated_flows-index-generator-Optional.of([2015-11-02T23:20:00.000Z/2015-11-02T23:21:00.000Z])	MAPREDUCE	60209
RUNNING	application_1442528378995_256344	aggregated_flows-index-generator-Optional.of([2015-11-02T23:18:00.000Z/2015-11-02T23:19:00.000Z])	MAPREDUCE	164729
FINISHED	application_1442528378995_253998	attacks-index-generator-Optional.of([2015-11-02T13:32:00.000Z/2015-11-02T13:33:00.000Z])	MAPREDUCE	47868
FINISHED	application_1442528378995_253997	sensor_stats-index-generator-Optional.of([2015-11-02T13:33:00.000Z/2015-11-02T13:34:00.000Z])	MAPREDUCE	24514

- Liste de tous les journaux collectés.

Figure 458: Liste des journaux collectés

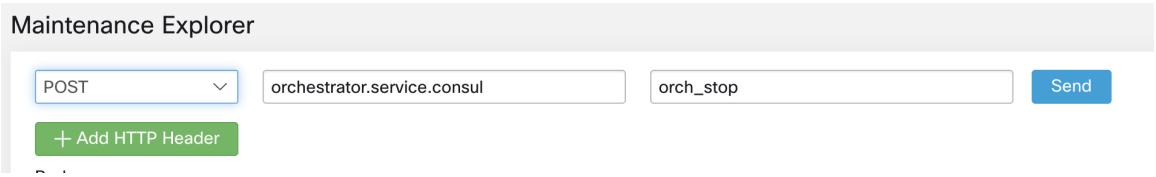


Utilisation du service d'instantané pour le débogage et l'entretien

Le service d’instantané peut être utilisé pour exécuter des commandes de service, mais il nécessite des privilèges de service d'assistance à la clientèle.

À l’aide de l’outil Explore (Explorer) (**Troubleshoot (Dépannage)** > **de l’explorateur de maintenance**), vous pouvez accéder à toute URI au sein de la grappe :

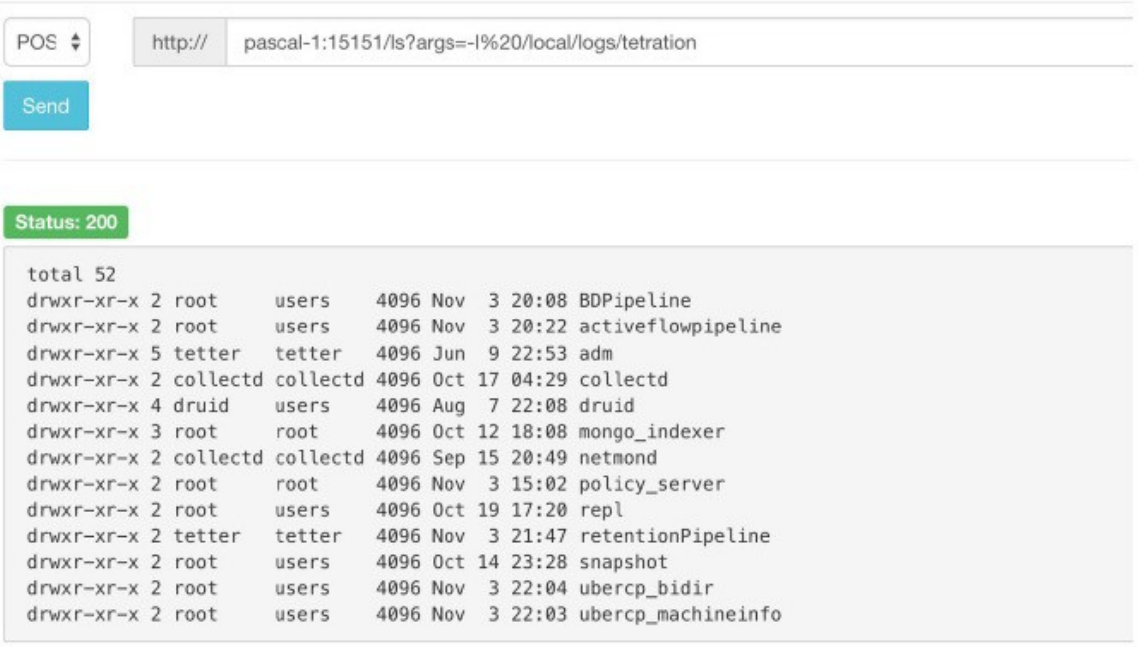
Figure 459: Service Snapshot (Instantané) pour le débogage et la maintenance



L’outil Explore (Explorer) ne s’affiche que pour les utilisateurs disposant de privilèges de service d'assistance à la clientèle.

Le service d’instantané s’exécute sur le port 15151 de chaque nœud. Il écoute uniquement sur le réseau interne (non accessible à l’extérieur) et possède des points terminaux POST pour diverses commandes.

Figure 460: Utilisation du service d'instantané pour le débogage et l'entretien



L'URI que vous devez atteindre est **POST** http://<nom d'hôte> : 15151/<cmd> ?args=<args>, où les arguments sont séparés par des espaces et codés en URI. Il n'exécute **pas** votre commande avec un shell. Cela empêcherait d'exécuter n'importe quelle opération.

Les points terminaux d'un instantané sont définis pour :

- **snapshot 0.2.5**

  –ls

  –**svstatus, svrestart - runs sv status, sv restart** Exemple :1.1.11.15:15151/svrestart?args=snapshot

  –hadoopls runs hadoop fs -ls <args>

  –hadoopdu - runs hadoop fs -du <args>

  Exemple pour **ps** : 1.1.11.31:15151/ps?args=eafux

  –du

  –ambari - runs ambari_service.py

  –monit

  –MegaCli64 (/usr/bin/MegaCli64)

  –service

  Hadoopfsck – exécute Hadoop -fsck

- **snapshot 0.2.6**

  –makecurrent - runs make -C /local/deploy-ansible current

  –netstat

- **snapshot 0.2.7 (exécuté en tant que UID « personne »)**

−cat

−head

queue

grep

−ip -6 neighbor

Adresse IP

−ip neighbor

Il existe un autre point terminal, POST /runsigned, qui exécutera les scripts Shell signés par Cisco Secure Workload. Il exécute gpg -d sur les données faisant l'objet d'un POST. Si cela peut être vérifié par rapport à une signature, le texte chiffré est exécuté dans un shell. Cela signifie l'importation d'une clé publique sur chaque serveur dans le cadre de la configuration d'Ansible et la nécessité de sécuriser la clé privée.

Guide de l'exécution

Les utilisateurs disposant de privilèges d'assistance client peuvent utiliser le répertoire en sélectionnant **Troubleshoot (Dépannage)** > **Maintenance Explorer (Explorateur d'entretien)** dans la barre de navigation dans la partie gauche de la fenêtre. Sélectionnez **POST** dans la liste déroulante. (Sinon, vous recevrez des erreurs Page introuvable lors de l'exécution des commandes).

Utilisation du point terminal REST d'instantané pour redémarrer les services :

- **druid: 1.1.11.17:15151/service?args=supervisord%20restart**
  - −Les hôtes druid ont tous des adresses IP 0.17 à .24; .17, .18 sont les coordonnateurs, .19 est l'indexeur et .20-.24 sont les intermédiaires
- **lanceurs de pipelines Hadoop :**
  - −1.1.11.25:15151/svrestart?args=activeflowpipeline
  - −1.1.11.25:15151/svrestart?args=adm
  - −1.1.11.25:15151/svrestart?args=batchmover_bidir
  - −1.1.11.25:15151/svrestart?args=batchmover_machineinfo
  - −1.1.11.25:15151/svrestart?args=BDPipeline
  - −1.1.11.25:15151/svrestart?args=mongo_indexer
  - −1.1.11.25:15151/svrestart?args=retentionPipeline
- **moteur de politique**
  - −1.1.11.25:15151/svrestart?args=policy_server
- **wss**
  - −1.1.11.47:15151/svrestart?args=wss

Présentation des points terminaux Explore ou Instantané

Pour exécuter un terminal, vous devez vous rendre à la page **Troubleshoot** > **Maintenance Explorer** (Dépannage > Explorateur de maintenance) à partir de la barre de navigation sur le côté gauche de la fenêtre.

Vous pouvez également afficher chaque présentation de chaque point terminal dans la page d'exploration en exécutant une commande **POST** sur n'importe quel hôte, telle que **<end- point>?usage=vrai**.

Par exemple : **makecurrent?usage=vrai**

Commandes get

Point d'accès	Description
bm_details	Affiche les informations sur les composants sans système d'exploitation
points terminaux	Répertorie tous les points terminaux sur l'hôte
members	Affiche la liste actuelle des membres consul, ainsi que leur statut
port2cimc	• Répertorie les adresses IP auxquelles le port est connecté • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
état	Affiche l'état du service d'instantané sur l'hôte
vm_info	• Affiche les informations sur la machine virtuelle de l'emplacement • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécutez le point terminal sous la forme **vm_info?args=<vmname>**

Commandes post

Table 46: Commandes post

Point d'accès	Description
bm_shutdown_or_reboot	• Arrêtez ou redémarrez progressivement un hôte sans système d'exploitation en commençant par arrêter toutes les machines virtuelles sur cet hôte, puis en exécutant une commande d'arrêt ou redémarrage de l'hôte sans système d'exploitation. Vous pouvez également obtenir l'état d'arrêt ou de redémarrage à l'aide de ce point terminal. • Pour obtenir l'état d'arrêt ou de redémarrage d'un nœud, utilisez : `bm_shutdown_or_reboot? query=serial=FCH2308V0FH` • Pour démarrer un arrêt progressif sans système d'exploitation, utilisez : `bm_shutdown_or_reboot? method=POST` et définissez le corps comme un objet JSON qui décrit le numéro de série de l'hôte. Par exemple : `{"serial": "FCH2308V0FH"}` • Pour effectuer un redémarrage progressif des machines sans système d'exploitation, utilisez : `bm_shutdown_or_reboot? method=POST` et définissez le corps comme un objet JSON qui décrit le numéro de série de l'hôte et comprend une clé de redémarrage définie sur « vrai ». Par exemple : `{"serial" : "FCH2308V0FH", "reboot" : vrai}`
cat	Commande d'encapsulation pour la commande *cat* Unix
cimc_password_random	• Rend aléatoire le mot de passe CIMC. • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
cleancmdlogs	Efface les journaux de `/local/logs/tetration/snapshot/cmdlogs/snapshot_cleancmdlogs_log`
clear_sel	• Efface les journaux des événements du système • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**

Point d'accès	Description
cluster_fw_upgrade	• Il s'agit d'une fonctionnalité **bêta** pour cette version. • Exécute une mise à niveau du micrologiciel UCS dans l'ensemble de la grappe. • Une fois cette opération terminée, chaque système sans système d'exploitation doit être redémarré pour activer le BIOS et les micrologiciels des autres composants. • Exécuter sous la forme : **cluster_fw_upgrade** • Ce point terminal lance et surveille la mise à niveau du micrologiciel et met à jour le fichier journal lorsqu'une étape de la mise à niveau a été commencée ou terminée. • Pour obtenir l'état de la mise à niveau, utilisez le point de terminaison **cluster_fw_upgrade_status**.
cluster_fw_upgrade_status	• Il s'agit d'une fonctionnalité **bêta** pour cette version. • Obtenez l'état de la mise à niveau complète du micrologiciel de l'UCS de la grappe. • Exécuter sous la forme **cluster_fw_upgrade_status**
cluster_powerdown	• Met la grappe hors tension. • *À utiliser avec prudence, car la grappe est désactivée*. • Exécutez le point terminal sous la forme `cluster_powerdown?args=-start`.
collector_status	• Affiche l'état du collecteur. • Il doit être exécuté sur les hôtes du collecteur uniquement.
consul_kv_export	• Affiche les paires k-v de cons au format JSON • Doit être exécuté uniquement sur les hôtes de l'orchestrateur.

Point d'accès	Description
consul_kv_recurse	• Affiche les paires k-v de consul sous forme de tableau • Doit être exécuté uniquement sur les hôtes de l'orchestrateur.
df	Commande d'encapsulation pour la commande *df* Unix
dig	Commande d'encapsulation pour la commande *dig* Unix
dmesg	Commande d'encapsulation pour la commande *dmesg* Unix
dmidecode	Commande d'encapsulation pour la commande Unix *dmidecode*
druid_coordinator_v1	Affiche les statistiques du druide.
du	Commande d'encapsulation pour la commande *du* Unix
dusorted	Commande d'encapsulation pour la commande *dusorted* Unix
Externalize_change_tunnel	• Modifie l'adresse IP du collecteur qui sera utilisée pour tunneliser l'interface utilisateur du contrôleur CIMC • Exécuter en tat que : **externalize_change_tunnel?method=POST** • Passer **{"collector_ip" : "<IP>"}** dans le corps • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
externalize_mgmt	• Affiche l'état de l'externalisation de l'interface utilisateur du contrôleur CIMC pour chaque serveur • Affiche l'adresse et le temps restant pour l'externalisation • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**

Point d'accès	Description
externalize_mgmt_read_only_password	• Modifie le mot de passe en lecture seule (ta_guest) pour le commutateur et l'interface utilisateur du contrôleur CIMC • Ne change que lorsqu'ils sont extériorisés. • Exécuter sous la forme : **externalize_mgmt_read_only_password?method=POST** • Passer **{"password" : "<password>"}** dans le corps • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
fsck	• Commande d'encapsulation pour la commande *fsck* Unix • Doit être exécuté uniquement sur **l'hôte sans système d'exploitation**
get_cimc_techsupport	• Saisissez l'adresse IP interne de la machine sans système d'exploitation. • Récupère l'offre groupée de soutien technique du contrôleur CIMC. • Une fois la commande achevée, le résultat peut être téléchargé à partir de la page des instantanés de l'interface utilisateur. • Elle peut être exécutée à partir de n'importe quel hôte de la grappe et nécessite l'adresse IP interne sans système d'exploitation comme argument. • Exemple : **get_cimc_techsupport?args=1.1.0.9**
syslog_endpoints	• Contrôle les configurations syslog pour un ou plusieurs serveurs UCS. • Exécutez la commande accompagnée de *-h* pour obtenir une liste complète des paramètres.
grep	Commande d'encapsulation pour la commande Unix *grep*
hadoopbalancer	• Distribue les données HDFS uniformément sur tous les nœuds • Doit être exécuté sur **des hôtes dotés de HDFS**. Par exemple, hôte de lancement

Point d'accès	Description
hadoopdu	• Imprime l'utilisation de répertoire de HDFS • Elle doit être exécutée sur **des hôtes dotés de HDFS**. Par exemple, hôte de lancement
hadoopfsck	• Exécute Hadoop fsck et signale l'état du système de fichiers HDFS fourni • Elle utilise également « -delete » (supprimer) comme argument pour effacer les blocs corrompus ou manquants. • Avant de supprimer, assurez-vous que tous les DataNodes sont actifs, sinon vous pourriez perdre des données • Doit être exécuté sur les hôtes de lancement uniquement. • Pour rapporter l'état qui est exécuté comme : `hadoopfsck?args=/raw` • Pour supprimer les fichiers corrompus, exécutez-la sous la forme : `hadoopfsck?args=/raw -delete`
hadoopls	• Répertorie le système de fichiers Hadoop • Doit être exécuté sur **des hôtes qui comportent HDFS**, par exemple l'hôte de lancement.
hbasehbck	• Vérifie les problèmes de cohérence et d'intégrité des tableaux et la réparation d'une HBase endommagée • Doit être exécuté **uniquement sur les hôtes HBase** • Pour identifier une incohérence, exécutez-la sous la forme : `hbasehbck?args=-details` • Pour réparer une HBase endommagée, exécutez-la sous la forme : `hbasehbck?args=-repair` • Le résultat figure dans /local/logs/tetration/snapshot/cmdlogs/snapshot_hasehbck_log.txt • *Réparez avec prudence*

Point d'accès	Description
hdfs_safe_state_recover	• Supprime HDFS de l'état sans échec • Requis si HDFS est en READ_ONLY_STATE (ÉTAT EN LECTURE) en raison de la capacité complète et que de l'espace a été libéré • Doit être exécuté sur les **hôtes de lancement uniquement** • Exécuter sous la forme : **hadoopfs-rm'{{ hdfs_safe_state_marker_location }}/HDFS_READ_ONLY'**
initctl	Commande d'encapsulation pour la commande *initctl* Unix
head	Commande d'encapsulation pour la commande *head* Unix
internal_haproxy_status	• Imprime l'état et les statistiques internes haproxy • Doit être exécuté **uniquement sur les hôtes de l'orchestrateur**
ip	Commande d'encapsulation pour la commande *ip* Unix
ipmifru	• Imprime des informations sur les unités remplaçables sur site (FRU) • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmilan	• Imprime la configuration du réseau local. • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmisel	• Imprime les entrées du journal des événements du système (SEL) • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
ipmisensorlist	• Imprime les informations du capteur IPMI • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
jstack	Imprime les traces de pile des threads (unités d'exécution) Java pour un processus Java ou un fichier central donné.

Point d'accès	Description
ls	Commande d'encapsulation pour la commande *ls* Unix
lshw	Commande d'encapsulation pour la commande *lshw* Unix
lsof	Commande d'encapsulation pour la commande *lsof* Unix
lvdisplay	Commande d'encapsulation pour la commande *lvdisplay* Unix
lvs	Commande d'encapsulation pour la commande *lvs* Unix
lvscan	Commande d'encapsulation pour la commande *lvscan* Unix
makecurrent	• Réinitialise ou accélère le pipeline qui traite le marqueur en fonction des horodatages actuels. • Doit être exécuté sur les **nœuds de l'orchestrateur uniquement** • Exécutez le point terminal en tant que **makecurrent?args=–start**
mongo_rs_status	• Affiche l'état de la duplication mongo • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore**
mongo_stats	• Affiche les statistiques mongo • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore**
mongodump	• Vide les collectes de la base de données • Doit être exécuté sur les hôtes **mongodb ou enforcementpolicystore** • Exécuter sous la forme : mongodump?args=<collection>[–db DB]
monit	Commande d'encapsulation pour la commande de *monit* Unix
namenode_jmx	Affiche les métriques jmx du nœud de nom principal

Point d'accès	Description
namenode_checkpoint	La vérification a lieu toutes les heures sur le nœud de nom en veille. Si `Namenode-1` ou `Secondarynamenode-1`est en panne pour maintenance pendant une longue période, l'état de service `NN_checkpoint` affiche **UNHEALTHY** (NON INTÈGRE). Une vérification manuelle est nécessaire pour effacer cette condition. Exécutez le POST `Namenode_checkpoint` sur le `launcherHost-1` (ou tout autre `launcherHost` en cours d'exécution). **Note** Si un point de reprise n'est pas effectué régulièrement, les journaux de modification maintenus par le service **journalnode** exécuté dans les instances de Zookeeper ne sont pas purgés et le disque risque d'être saturé.
namenode_failover	Avant d'exécuter **UPGRADE** (METTRE À NIVEAU) ou **REBOOT** (REDÉMARRER), assurez-vous d'exécuter la vérification préalable à la mise à niveau. Si le service `Namenode` n'est pas en cours d'exécution, vous pouvez rencontrer une erreur de vérification de l'intégrité du service avec le message suivant : « `Failed: (Namenode service on NN-1/check) namenode.service.consul and namenode-1.node.consul resolve differently.` (Échec : (Service Namenode sur NN-1/check) namenode.service.consul et namenode-1.node.consul se résolvent différemment). »
namenodeha_get_details	Affiche l'état actuel **ACTIVE** (ACTIF) ou **STANDBY** (VEILLE) pour chaque instance de `namenode` (nom de nœud). Si le service d'instance est en panne ou si le service `namenode` n'est pas en cours d'exécution sur l'instance, l'état affiche **DOWN** (EN PANNE).
ndisc6	Commande d'encapsulation pour la commande *ndisc6* Unix
netstat	Commande d'encapsulation pour la commande *netstat* Unix
ntpq	Commande d'encapsulation pour la commande *ntpq* Unix

Point d'accès	Description
orch_reset	• Réinitialise l'état de l'orchestrateur à IDLE (INACTIF) • Exécuter après un échec de mise en service ou de désactivation • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **N'utilisez pas cette commande sans consulter le service d'assistance à la clientèle**
orch_stop	• Arrête l'orchestrateur principal et déclenche un basculement • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **UTILISER AVEC PRÉCAUTION**
ping	Commande d'encapsulation pour la commande *ping* Unix
ping6	Commande d'encapsulation pour la commande *ping6* Unix
ps	Commande d'encapsulation pour la commande *ps* Unix
pv	Commande d'encapsulation pour la commande *pv* Unix
pvs	Commande d'encapsulation pour la commande *pvs* Unix
pvdisplay	Commande d'encapsulation pour la commande *pvdisplay* Unix
rdisc6	Commande d'encapsulation pour la commande *rdisc6* Unix
rebootnode	• Redémarre le nœud • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement**
recover_rpmdb	• Récupère un RPMDB endommagé sur un nœud • Peut être exécuté sur des machines sans système d'exploitation ou des machines virtuelles

Point d'accès	Description
recoverhbase	• Récupère le service HBase et TSDB • Doit être exécuté sur **les hôtes de l'orchestrateur uniquement** • Doit être exécuté lorsque HDFS est à l'état intègre
recovervm	• Essayer de récupérer la machine virtuelle via la commande stop/fsck/start • Doit être exécuté sur **les hôtes de l'orchestrateur uniquement** • Exécutez le point terminal ainsi **recovervm?args=<vmname>**
restartservices	• Arrête et démarre tous les services non liés à l'interface utilisateur • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • **UTILISER AVEC PRÉCAUTION** • Exécutez le point terminal sous la forme **restartservices?args=–start**
runsigned	• Exécute le script signé fourni par Cisco • Suivez les étapes fournies dans les instructions relatives au script
service	Commande d'encapsulation pour la commande de *service* Unix
smartctl	• Exécutez l'exécutable smartctl • Ne doit être exécuté que sur un nœud sans système d'exploitation
storcli	Commande d'encapsulation pour la commande *storcli* Unix
sudocat	Emballage pour la commande *cat* qui fonctionne uniquement sous /var/log ou /local/logs
sudogrep	Commande d'encapsulation pour la commande *grep* qui fonctionne uniquement sous /var/log ou /local/logs

Point d'accès	Description
sudohead	Commande d'encapsulation pour la commande « head » qui fonctionne uniquement sous /var/log ou /local/logs
sudols	Commande d'encapsulation pour la commande « ls » qui fonctionne uniquement sous /var/log ou /local/logs
sudotail	Commande d'encapsulation pour la commande « tail » qui fonctionne uniquement sous /var/log ou /local/logs
sudozgrep	Commande d'encapsulation pour la commande « zgrep » qui fonctionne uniquement sous /var/log ou /local/logs
sudozcat	Commande d'encapsulation pour la commande « zcat » qui fonctionne uniquement sous /var/log ou /local/logs
svrestart	Redémarre le service saisi. Exécutez la commande sous la forme `svrestart?args=<servicename>`
svstatus	Imprime l'état du service saisi, exécutez-le sous la forme `svstatus?args=<servicename>`
switchinfo	Obtenir des renseignements sur les commutateurs de la grappe.
switch_namenode	• Basculement manuel du nœud désigné par le nom du nœud principal ou secondaire • Doit être exécuté sur l'hôte **orchestrator.service.consul** uniquement • Exécuter lors de la remise en service ou de la désactivation des hôtes de nœud de nom • Exécutez le point terminal sous la forme **switch_namenode?args=--start**
switch_secondarynamenode	• Basculement manuel du nœud désigné par le nom secondaire du nœud secondaire au nœud principal • Doit être exécuté sur l'hôte **orchestrator.service.consul** uniquement • Exécuter lors de la remise en service ou de la désactivation des hôtes de nœud de nom • Exécuter le point terminal sous la forme **switch_secondarynamenode?args=--start**

Point d'accès	Description
switch_yarn	• Basculement manuel du gestionnaire de ressources à partir du serveur principal ou secondaire, ou inversement • Doit être exécuté sur l'**hôte orchestrator.service.consul uniquement** • Exécuter lors de la désactivation ou de la désactivation des hôtes du gestionnaire de ressources • Exécuter le point terminal sous la forme **switch_yarn?args=–start**
tail	Commande d'encapsulation pour la commande *tail* Unix
toggle_chassis_locator	• Activez ou désactivez un localisateur de châssis sur une base physique sans système d'exploitation spécifiée par le numéro de série du nœud. • Exécuté à partir de n'importe quel nœud sous la forme : **toggle_chassis_locator?method=POST** • Définissez dans le corps du texte un objet JSON qui décrit le numéro de série de l'hôte (un seul numéro de série à la fois est pris en charge), par exemple : **{"serials": ["FCH2308V0FH"]}**
tnp_agent_logs	• Créer un instantané de tous les fichiers journaux fournis par les agents de l'équilibreur de charge enregistrés en tant qu'orchestrateurs externes • Doit être exécuté sur les hôtes du serveur de lancement
tnp_datastream	• Créer un instantané avec les données de flux de politique utilisées par les agents d'application de la politique de l'équilibreur de charge enregistrés en tant qu'orchestrateurs externes • Doit être exécuté sur les hôtes de l'orchestrateur • Pour télécharger les données de flux d'état des politiques, exécutez le point terminal sous la forme **tnp_datastream?args=–ds_type datasink**
ui_haproxy_status	Imprime les statistiques et l'état haproxy pour l'haproxy externe

Point d'accès	Description
uptime	Commande d'encapsulation pour la commande *uptime* Unix
userapps_kill	• Arrête toutes les applications utilisateur en cours d'exécution • Doit être exécuté **uniquement sur les hôtes du lanceur**
vgdisplay	Commande d'encapsulation pour la commande *vgdisplay* Unix
vgs	Commande d'encapsulation pour la commande *vgs* Unix
vmfs	• Répertorie le système de fichiers sur une machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmfs?args=<vmname>**
vminfo	• Imprime les informations de la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vminfo?args=<vmname>**
vmlist	• Listes de toutes les machines virtuelles sur un système sans système d'exploitation • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point de terminaison sous la forme **vmlist?args=<vmname>**
vmreboot	• Redémarre la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmreboot?args=<vmname>**

Point d'accès	Description
vmshutdown	• Arrêter progressivement la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sus la forme **vmshutdown?args=<vmname>**
vmstart	• Démarre la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmstart?args=<vmname>**
vmstop	• Forcer l'arrêt de la machine virtuelle • Doit être exécuté sur les **hôtes sans système d'exploitation uniquement** • Exécuter le point terminal sous la forme **vmstop?args=<vmname>**
yarnkill	• Arrête une application Yarn en cours d'exécution • Doit être exécuté **uniquement sur les hôtes du lanceur** • Exécuter le point terminal sous la forme **yarnkill?args=<application id>** • Pour arrêter toutes les applications, exécutez-le sous la forme **yarnkill?args=ALL**
yarnlogs	• Vide les 500 derniers Mo de journaux d'application yarn • Doit être exécuté **uniquement sur les hôtes du lanceur** • Exécuter le point terminal sous la forme **yarnlogs?args=<application id> <job user>**
zcat	Commande d'encapsulation pour la commande *zcat* Unix
zgrep	Commande d'encapsulation pour la commande *zgrep* Unix

Entretien du serveur

L'entretien du serveur implique le remplacement de tout composant défectueux, comme le disque dur, la mémoire ou le remplacement du serveur lui-même.

Note Si plusieurs serveurs de la grappe ont besoin d'être maintenus, procédez à leur entretien l'un après l'autre. La désactivation de plusieurs serveurs en même temps peut entraîner une perte de données.

Pour effectuer toutes les étapes de l'entretien d'un serveur, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Cluster Status(État de la grappe)** . Tous les utilisateurs y accèdent, mais les actions peuvent être effectuées par les utilisateurs du **service d'assistance à la clientèle** uniquement. Il affiche l'état de tous les serveurs physiques du support Cisco Cisco Secure Workload.

Figure 461: Entretien du serveur

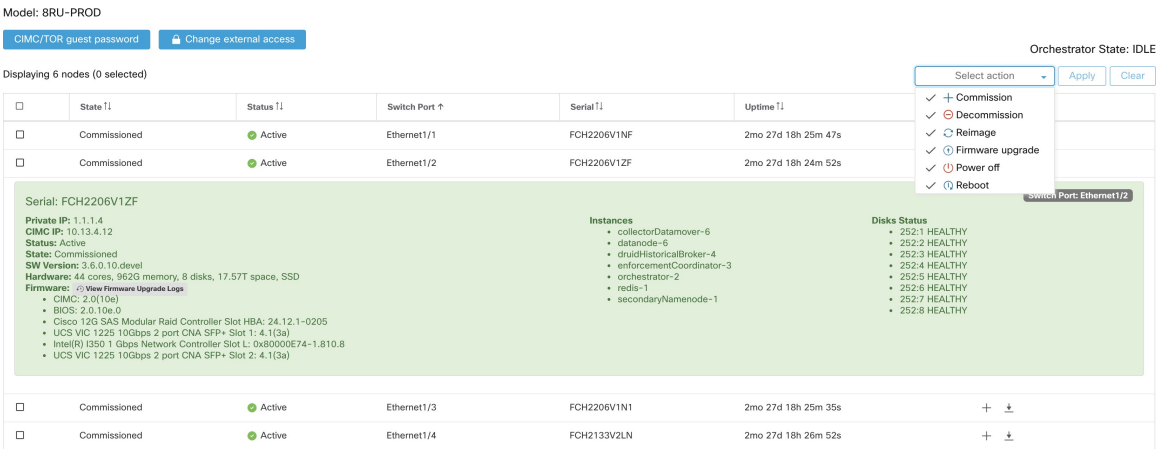
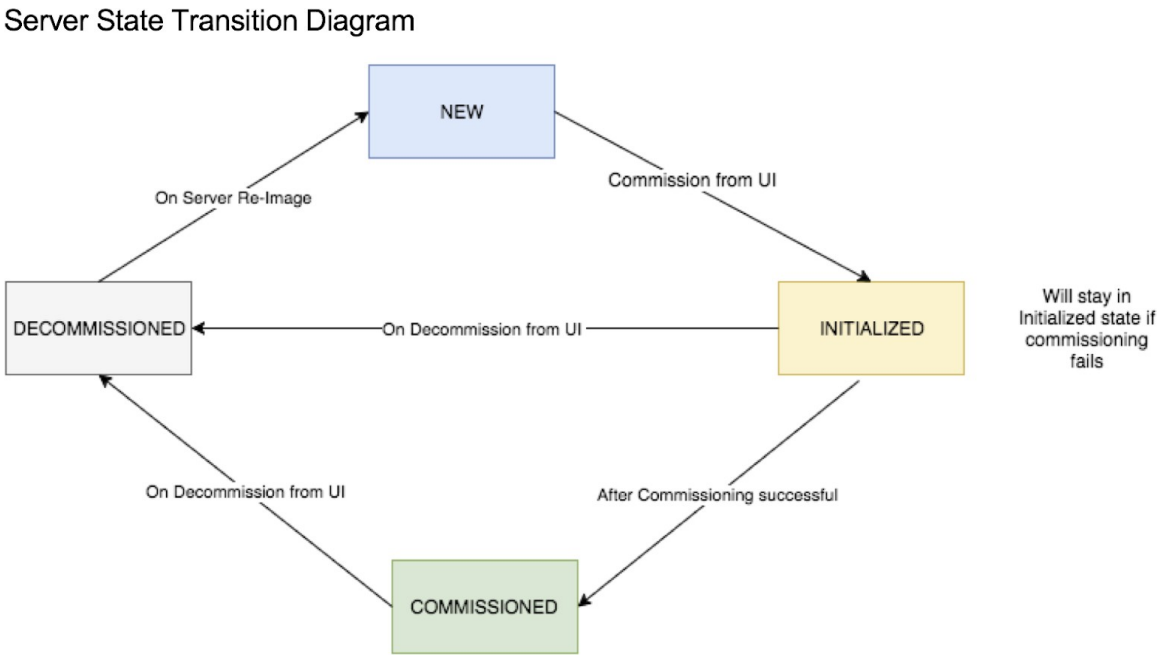


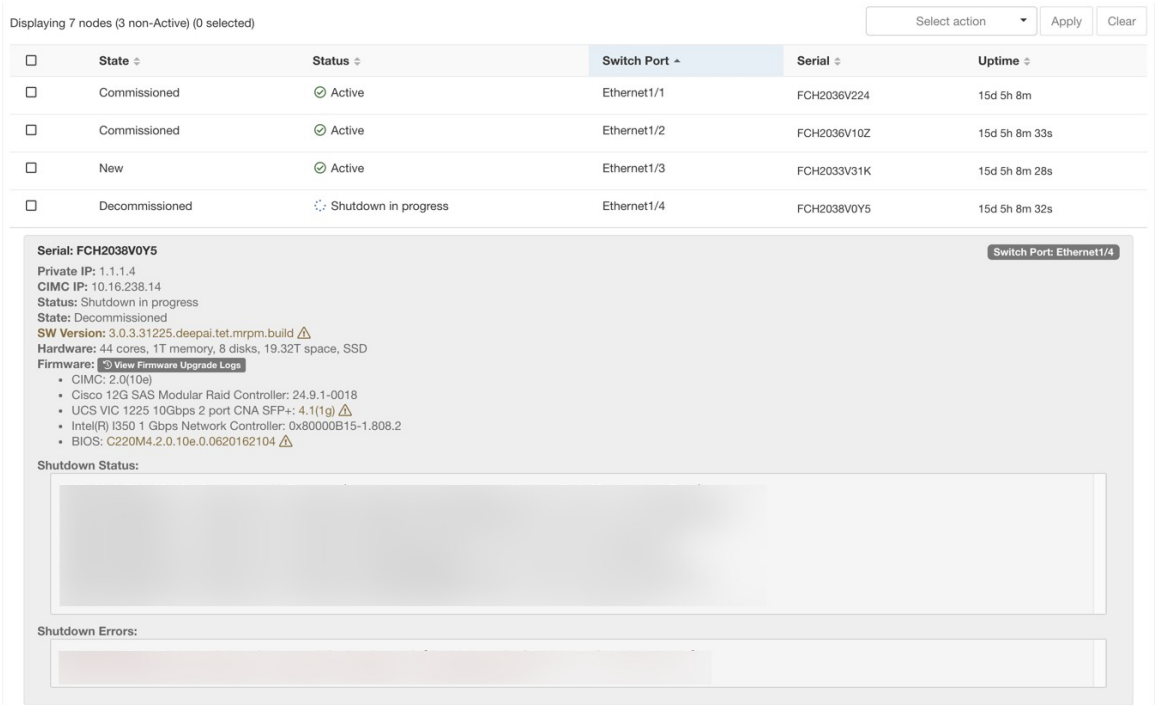
Figure 462: Diagramme de transition d'état du serveur



Étapes nécessaires pour remplacer un serveur ou un composant

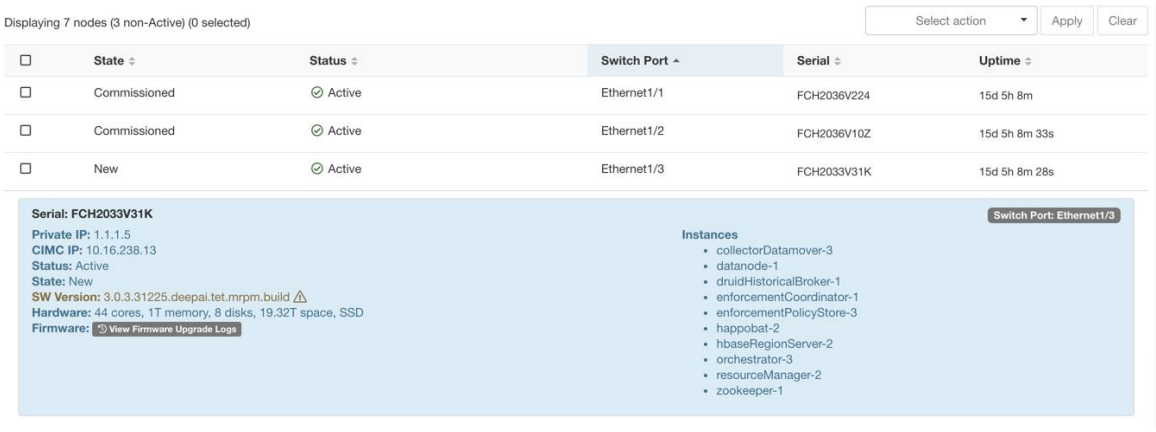
- **Déterminer le serveur qui nécessite une maintenance** : cela peut être fait en utilisant le numéro de *série* du serveur ou le *port de commutation* auquel le serveur est connecté, dans la page *Cluster Status* (État de la grappe). Notez l'adresse IP CIMC du serveur à remplacer. Elle est affichée dans la zone server (serveur) de la page *Cluster Status* (État de la grappe).
- **Vérifier les actions pour les machines virtuelles spéciales** : dans les zones serveur, recherchez les machines virtuelles ou les instances présentes sur le serveur et vérifiez si des actions spéciales doivent être effectuées pour ces machines virtuelles. La section suivante répertorie les actions pour les machines virtuelles pendant l'entretien du serveur.
- **Désactiver le serveur** : lorsque des actions préalables à la mise hors service sont effectuées, utiliser la page **Cluster Status** (État de la grappe) pour désactiver le serveur. Même si le serveur est en panne et semble *inactif* sur la page, vous pouvez toujours effectuer toutes les étapes d'entretien du serveur. Les étapes de désactivation peuvent être effectuées même si le serveur est hors tension.

Figure 463: Désactiver le serveur.



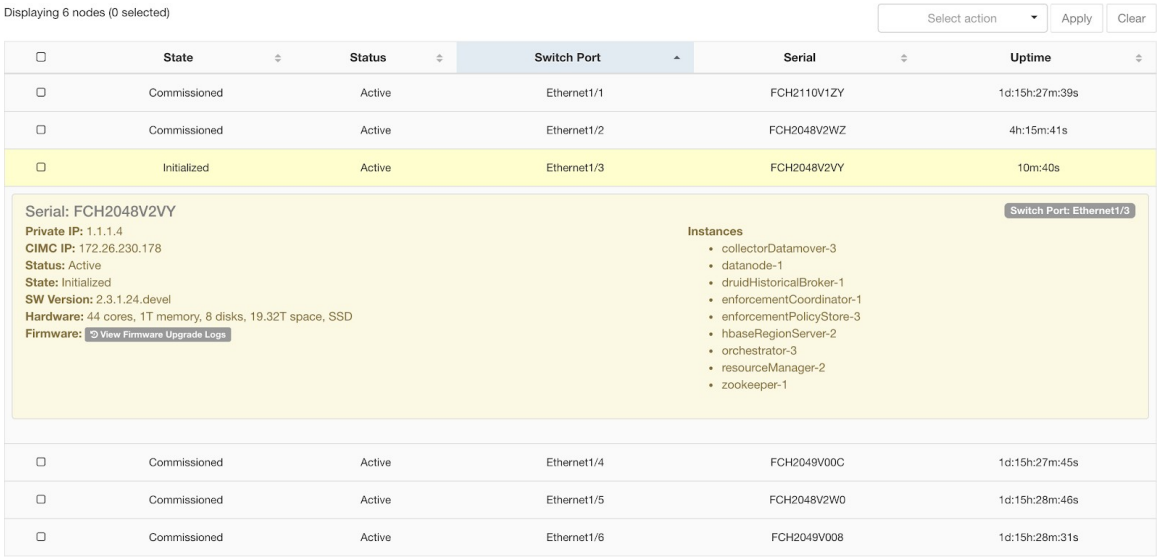
1. **Effectuez l'entretien du serveur** : une fois que le nœud est marqué *Decommissioned* (mis hors-service) dans la page **Cluster Status**, (État de la grappe) effectuez toutes les actions spéciales postérieures à la désactivation des machines virtuelles. Tout remplacement de composant ou de serveur peut être effectué dès maintenant. Si le serveur entier est remplacé, modifiez l'adresse IP du contrôleur CIMC du nouveau serveur pour qu'elle corresponde à celle du serveur remplacé. L'adresse IP du contrôleur CIMC de chaque serveur est indiquée dans la page **Cluster Status** (État de la grappe).
2. **Recréer l'image après le remplacement de composant** : Réinitialisez le serveur après le remplacement de composant à l'aide de la page **Cluster Status** (État de la grappe). La recréation de l'image prend environ 30 minutes et nécessite un accès CIMC aux serveurs. Le serveur est marqué *NEW* (NOUVEAU) une fois la recréation d'image terminée.
3. **Remplacement entier du serveur** : si le serveur en totalité est remplacé, il apparaîtra à l'état *NEW* (NOUVEAU) dans la page **Cluster Status** (État de la grappe). La version du logiciel du serveur est visible sur la même page. Si la version du logiciel est différente dans la version de la grappe, recréez l'image du serveur.

Figure 464: Remplacement du serveur



4. **Mettre en service le serveur** : une fois que le serveur est marqué *NEW* (NOUVEAU), nous pouvons lancer la mise en service du nœud à partir de la page **Cluster Status** (État de la grappe). Cette étape met en service les machines virtuelles sur le serveur. La mise en service d'un serveur prend environ 45 minutes. Le serveur sera marqué « *Commissioned* » (mis en service) une fois la mise en service terminée.

Figure 465: Mettre le serveur en service

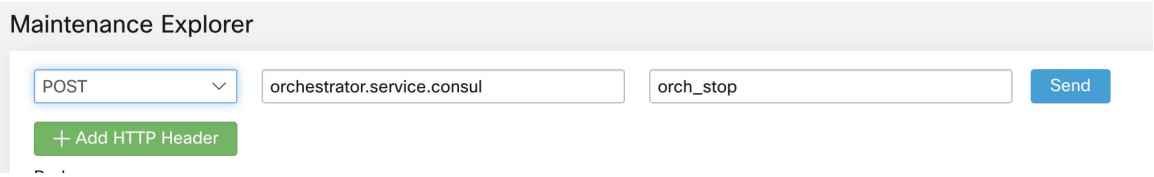


Actions sur les machines virtuelles pendant l'entretien du serveur

Certaines machines virtuelles nécessitent des actions spécifiques pendant la procédure d'entretien du serveur. Ces actions peuvent être préalables, se situer après la mise hors-service, ou après la mise en service.

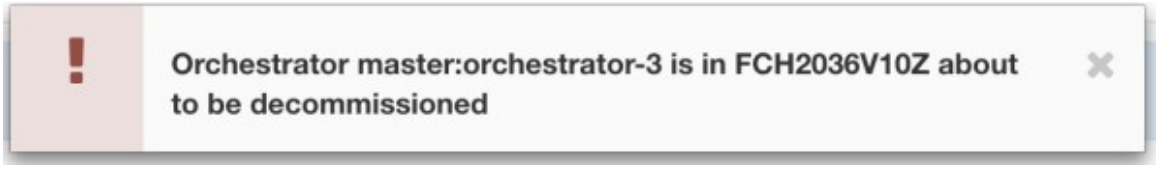
- **Orchestrateur principal** : il s'agit d'une action préalable à la mise hors-service. Si le serveur faisant l'objet d'entretien est doté d'un Orchestrateur principal, exécutez la commande POST *orch_ stop* sur orchestrator.service.consul à partir de la page d'exploration avant de procéder à la mise hors-service. Cela commute l'orchestrateur principal.

Figure 466: Explorateur de maintenance



Si vous essayez de désactiver un serveur doté d'un orchestrateur principal, l'erreur suivante s'affiche.

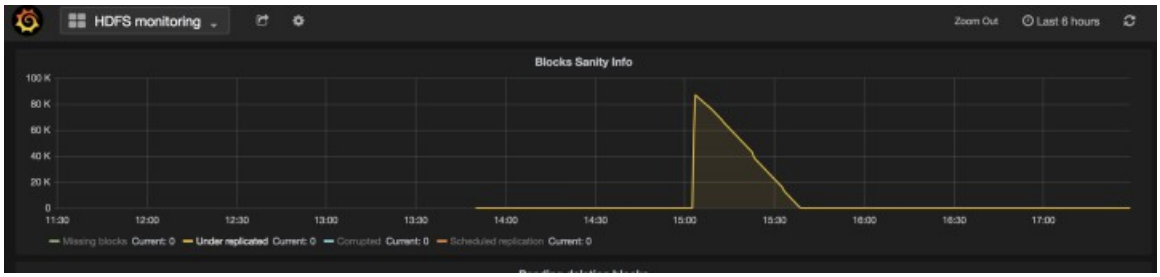
Figure 467: Désactiver un serveur avec une erreur d'orchestrateur principal



Pour déterminer l'orchestrateur principal, exécutez la commande explore `primaryorchestrator` sur n'importe quel hôte.

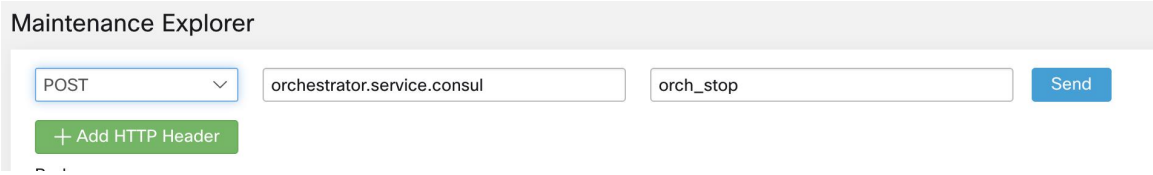
- **Namenode** : Si le serveur en cours d'entretien contient une machine virtuelle (namenode), exécutez la commande POST *switch_namenode* sur orchestrator.service.consul à partir de la page explore après la désactivation, puis la commande POST *switch_namenode* sur orchestrator.service.consul après la mise en service. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Secondary namenode** : Si le serveur en cours d'entretien comporte une VM secondaire, alors exécutez la commande POST *switch_secondarynamenode* sur orchestrator.service.consul à partir de la page explore après la désactivation, puis la commande POST *switch_ Secondarynamenode* sur orchestrator.service.consul après la mise en service. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Resource Manager primary** : si le serveur en cours d'entretien est doté du gestionnaire de ressources principal, exécutez la commande POST *switch_yARN* sur orchestrator.service.consul à partir de la page d'exploration. Il s'agit d'actions postérieures à la désactivation et à la mise en service.
- **Datanode** : la grappe ne tolère qu'une seule défaillance Datanode à la fois. Si plusieurs serveurs contenant des machines virtuelles Datanode ont besoin d'être entretenus, effectuez l'entretien du serveur un à la fois. Après chaque entretien de serveur, attendez que le tableau sous Surveillance | hawkeye | hdfs-monitoring | Block Sanity Info, Missing blocks et Under replicated couts (Informations sur la sécurité des blocs, blocs manquants et nombre de réplications insuffisant) soit à 0.

Figure 468: Maintenance du serveur : nœud de données



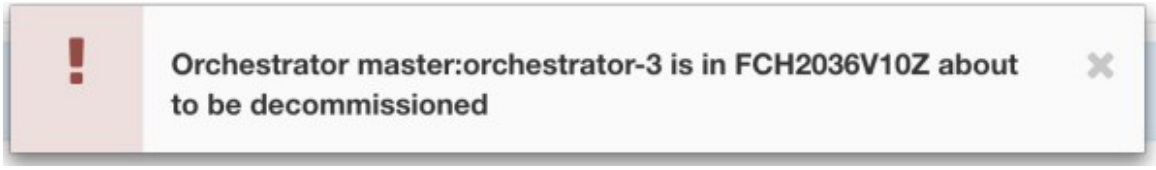
- **Orchestrateur principal** : il s'agit d'une action préalable à la mise hors-service. Si le serveur faisant l'objet d'entretien est doté d'un Orchestrateur principal, exécutez la commande POST *orch_ stop* sur orchestrator.service.consul à partir de la page d'exploration avant de procéder à la mise hors-service. Cela commute l'orchestrateur principal.

Figure 469: Explorateur de maintenance



Si vous essayez de désactiver un serveur doté d'un orchestrateur principal, l'erreur suivante s'affiche.

Figure 470: Désactiver un serveur avec une erreur d'orchestrateur principal



Pour déterminer l'orchestrateur principal, exécutez la commande explore `primaryorchestrator` sur n'importe quel hôte.

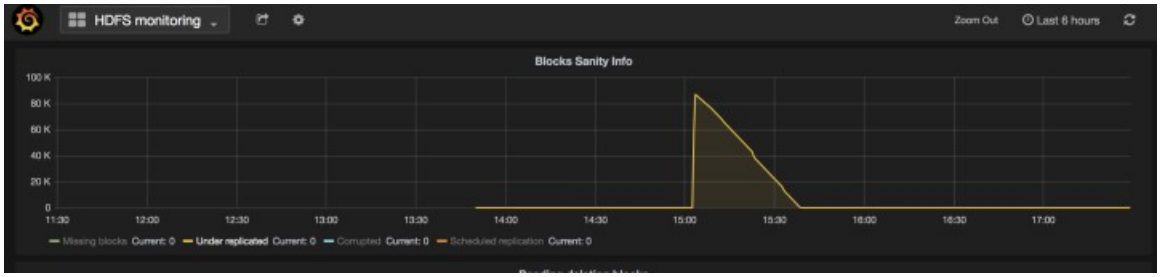
- **Namenode** : Si le serveur en cours d'entretien comporte une machine virtuelle Namenode, vérifiez que l'instance secondaryNamenode-1 est en cours d'exécution et que le service Namenode est actif. Exécutez la commande Explore POST `namenodeha_get_details` sur launcherHost-1 ou tout autre hôte launcherHosts en cours d'exécution, pour vérifier l'état. L'état SecondaryNamenode-1 doit être **Actif** ou **En attente**. Ne pas procéder à la désactivation si SecondaryNamenode-1 n'est pas à l'état **Actif** ou **En attente**.

- **Secondarynamenode** : si le serveur en cours d'entretien comporte une machine virtuelle secondarynamenode, vérifiez que l'instance namenode-1 est en cours d'exécution et que le service namenode est actif. Exécutez la commande Explore POST `namenodeha_get_details` sur launcherHost-1 ou tout autre hôte launcherHosts en cours d'exécution, pour vérifier l'état. L'état de namenode-1 doit être soit **Actif**, soit **En veille**. Ne procédez pas à la désactivation si `namenode-1` n'est pas à l'état **Actif** ou **En veille**.

- **Resource Manager primary** : si le serveur en cours d'entretien est doté du gestionnaire de ressources principal, exécutez la commande POST *switch_yARN* sur orchestrator.service.consul à partir de la page d'exploration. Il s'agit d'actions postérieures à la désactivation et à la mise en service.

- **Datanode** : la grappe ne tolère qu'une seule défaillance Datanode à la fois. Si plusieurs serveurs contenant des machines virtuelles Datanode ont besoin d'être entretenus, effectuez l'entretien du serveur un à la fois. Après chaque entretien de serveur, attendez que le tableau sous Surveillance | hawkeye | hdfs-monitoring | Block Sanity Info, Missing blocks et Under replicated couts (Informations sur la sécurité des blocs, blocs manquants et nombre de réplications insuffisant) soit à 0.

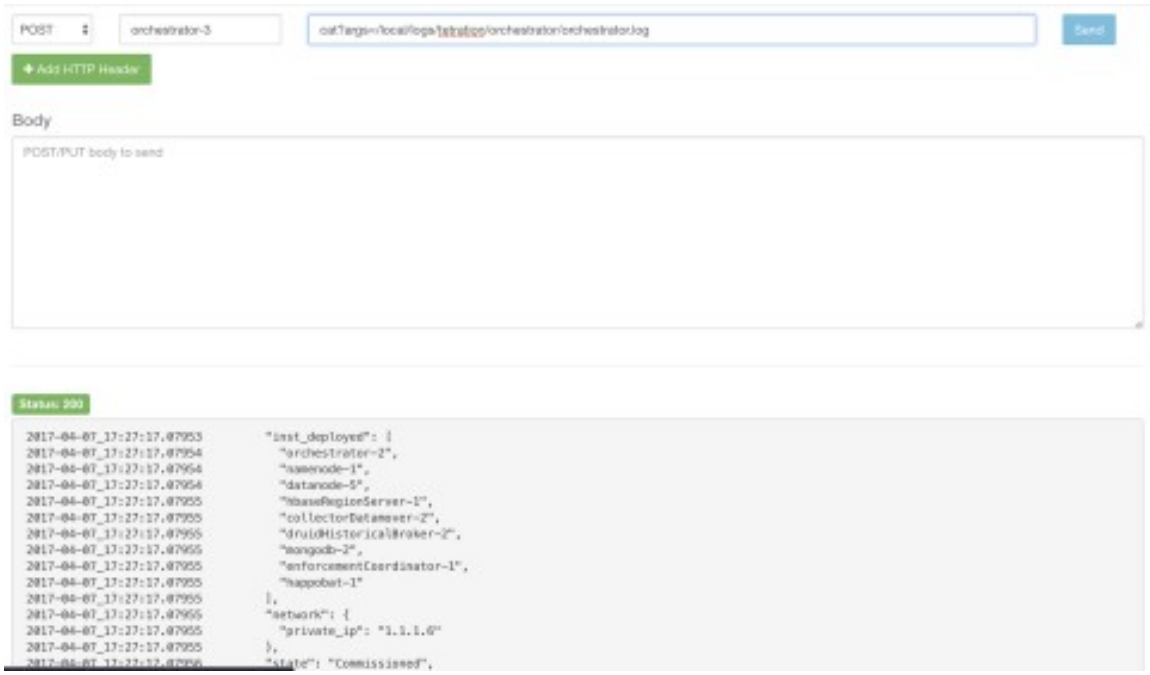
Figure 471: Maintenance du serveur : nœud de données



Dépannage de l'entretien du serveur

- **Journaux** : tous les journaux d'entretien du serveur font partie du journal de l'orchestrateur. L'emplacement est `/local/logs/tetration/orchestrator/orchestrator.log` sur orchestrator.service.consul.

Figure 472: Journal d'entretien du serveur



- **Mise hors service**
  - Cette étape supprime les machines virtuelles ou les instances sur le serveur.
  - Il supprime ensuite l'entrée de ces instances dans les tables de consul principales (backend).
  - Cette étape prend environ 5 minutes.
  - Le serveur sera marqué comme *Désactivé* une fois l'étape terminée.

Note Désactivé ne signifie pas que le serveur est éteint. La désactivation supprime uniquement le contenu Cisco Secure Workload sur le serveur.

- Si le serveur est éteint, il sera indiqué comme **Inactif**. Nous pouvons toujours exécuter la désactivation sur ce serveur à partir de la page d'état de la grappe. Mais l'étape de suppression des machines virtuelles ne s'exécutera pas, car le serveur est hors tension. Assurez-vous que ce serveur ne rejoint pas la grappe à l'état hors service. Il doit être recréé et rajouté à la grappe.

- **Recréation d'image**
  - Cette étape installe le système d'exploitation de base Cisco Secure Workload ou le système d'exploitation de l'hyperviseur sur le serveur.
  - Elle formate également les disques durs et installe quelques bibliothèques Cisco Secure Workload sur le serveur.
  - La fonction Reimage (recréation d'image) exécute un script appelé **mjolnir** pour lancer la création d'image du serveur. L'exécution de mjolnir prend environ 5 minutes, après quoi la création d'image commence. La création d'image prend environ 30 minutes. Les journaux pendant la création d'image peuvent uniquement être consultés sur la console du serveur en cours de recréation. L'utilisateur peut utiliser la clé ta_dev pour vérifier des informations supplémentaires sur la recréation, comme les journaux /var/log/nginx lors du démarrage pxe, /var/log/messages pour vérifier l'adresse IP DHCP et les configurations de démarrage pxe.
  - La recréation d'image nécessite une connectivité de contrôleur CIMC de l'orchestrateur. Le moyen le plus simple de vérifier la connectivité du contrôleur CIMC est d'utiliser la page explore et la commande POST ping?args=<cimc ip> à partir de orchestrator.service.consul. **N'oubliez** pas de modifier l'adresse IP du contrôleur CIMC dans le cas où le serveur est remplacé et de définir le mot de passe du contrôleur CIMC au mot de passe par défaut
  - De plus, le réseau CIMC aurait dû être défini dans les renseignements du site lors du déploiement de la grappe afin que les commutateurs soient configurés avec les bons routages. Dans le cas où la connectivité du contrôleur CIMC de grappe n'est pas définie correctement, vous verrez le résultat suivant dans les journaux de l'orchestrateur.

- **Mise en service**
  - Les programmes de mise en service des machines virtuelles sur le serveur et les guides d'exécutions dans les machines virtuelles pour installer le logiciel Cisco Secure Workload.
  - La mise en service dure environ 45 minutes.
  - Le flux de travail est similaire à un déploiement ou à une mise à niveau.
  - Les journaux indiquent les défaillances survenues lors de la mise en service.
  - Le serveur sur la page d'état de la grappe ne sera initialisé lors de la mise en service et marqué comme Mis en service qu'après que vous ayez terminé les étapes.

Exclure les systèmes sans système d'exploitation : bmexclude

Si une défaillance matérielle est détectée au redémarrage d'une grappe après une panne de courant, la grappe reste bloquée dans un état où nous ne pouvons ni exécuter le flux de travail de redémarrage pour obtenir des services stables, ni exécuter le flux de travail de mise en service, car l'arrêt des services entraîne un échec de la mise en service. Cette fonction devrait être utile dans de tels scénarios en permettant à l'utilisateur de redémarrer (mise à niveau) avec un matériel défectueux, après quoi le processus RMA habituel pour le système sans système d'exploitation défectueux peut être exécuté.

L'utilisateur doit utiliser un POST pour examiner le point terminal avec le numéro de série du système sans système d'exploitation à exclure :

1. Action : POST
2. Hôte : orchestrator.service.consul
3. Point terminal : exclude_bms?method=POST
4. Corps du texte : {"baremetal": ["BMSERIAL"]}

L'orchestrateur effectue quelques vérifications pour déterminer si l'exclusion est faisable. Auquel cas, il configure quelques clés consul et renvoie un message de réussite indiquant quelles machines sans système d'exploitation et quelles machines virtuelles seront exclues du prochain flux de travail de redémarrage ou de mise à niveau. Si les systèmes sans système d'exploitation comprennent certaines machines virtuelles, elles ne peuvent pas être exclues, comme décrit dans la section sur les limites ci-dessous. Le point terminal explore répond par un message indiquant pourquoi l'exclusion n'est pas possible. Après le POST réussi sur le point terminal explore, l'utilisateur peut lancer le redémarrage ou la mise à niveau au moyen de l'interface graphique principale et procéder au redémarrage habituel. À la fin de la mise à niveau, nous supprimons la liste bm d'exclusion. S'il est nécessaire d'exécuter la mise à niveau ou de redémarrer à nouveau avec les machines sans SE exclues, les utilisateurs doivent de nouveau effectuer un POST sur le point de terminaison bmexclude explore.

Restrictions

Les machines virtuelles suivantes ne peuvent pas être exclues :

- namenode
- secondaryNamenode
- mongodb
- mongodbArbiter

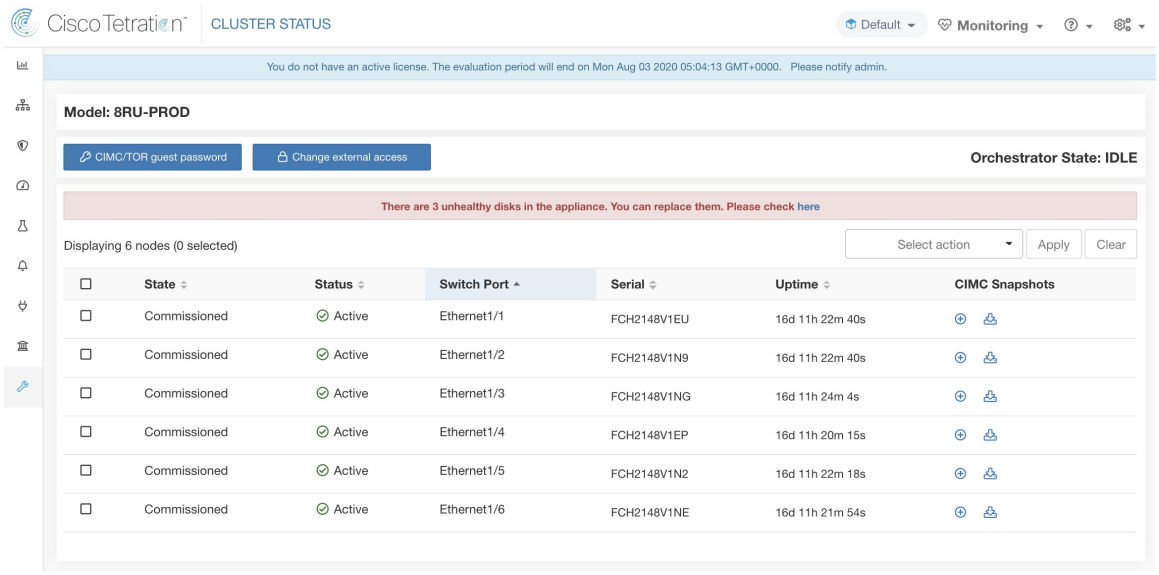
Entretien des disques

L'entretien des disques comprend le remplacement de tout disque dur défectueux sur un ou plusieurs serveurs. L'orchestrateur surveille l'intégrité des disques signalée par bmmgr sur chaque serveur de la grappe. S'il y a des disques défectueux, une bannière indique l'erreur dans la page **Cluster Status** (État de la grappe). Dans le volet de navigation, choisissez **Troubleshoot(Dépannage)** > **Cluster Status (État de la grappe)**.

La bannière affiche le nombre de disques qui sont dans un état **UNHEALTHY (NON INTÈGRE).** Cliquez *ici* sur la bannière, vous mènera à l'assistant de remplacement de disque. Vous ne pouvez qu'accéder à la page

de remplacement des disques, mais, à l'aide de l'assistant, le **service d'assistance à la clientèle** peut effectuer toutes les étapes nécessaires à l'entretien des disques.

Figure 473: Bannière de disque défectueux

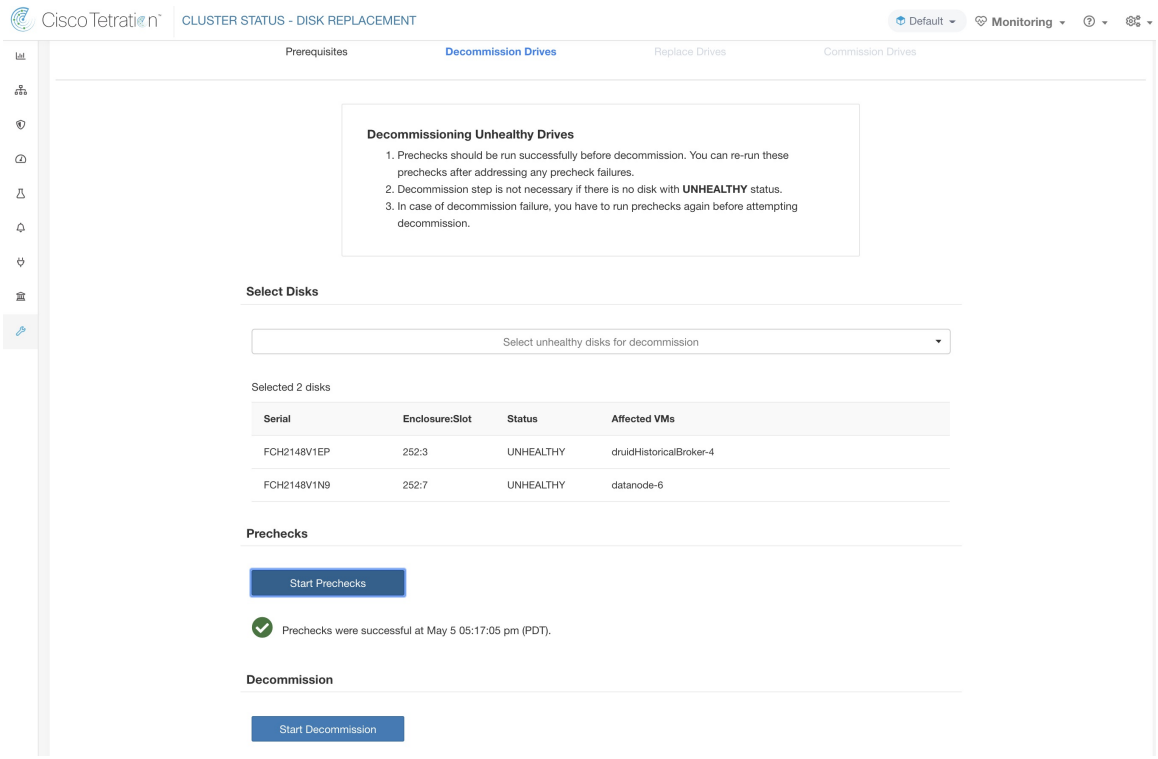


Vérifications préalables des exigences

Avant d'effectuer la désactivation ou la mise en service des disques, diverses vérifications sont effectuées au niveau du serveur de gestion. Toutes les vérifications doivent être réussies avant que vous puissiez procéder à la désactivation ou à la mise en service des disques.

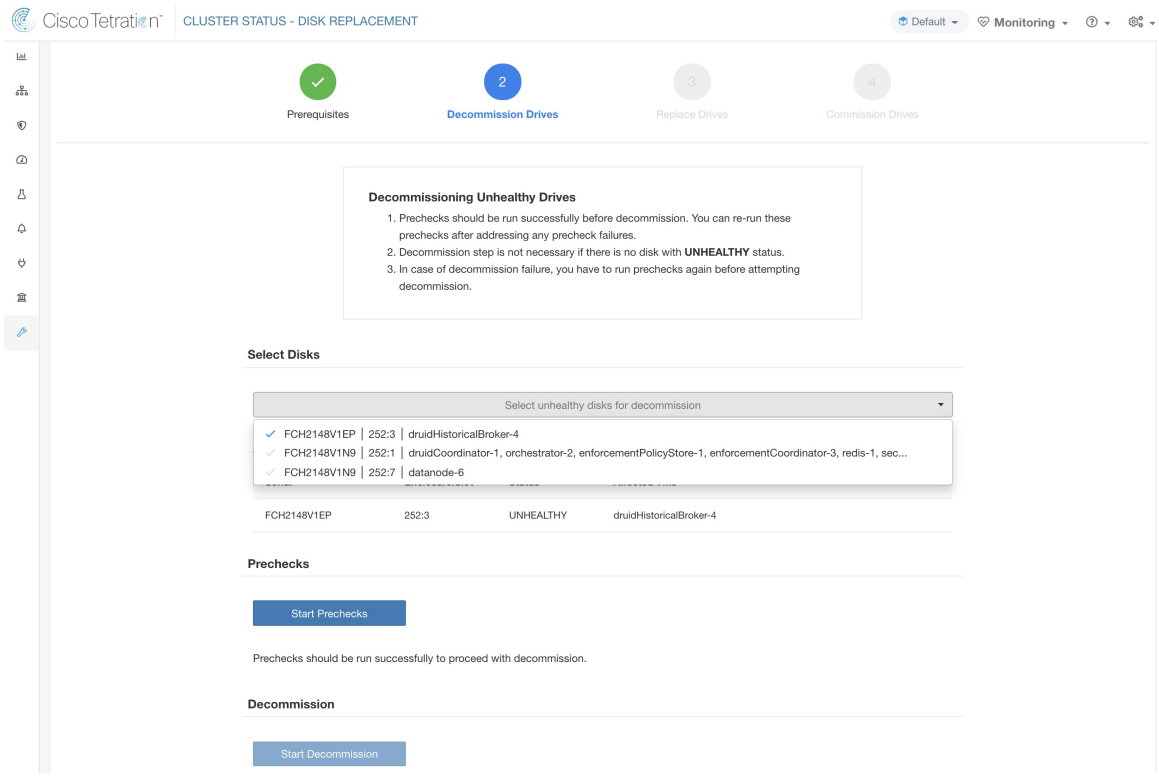
LLes vérifications infructueuses sont signalées dans **l'assistant de remplacement de disque** avec les détails de l'échec et les mesures correctives à prendre avant de passer à l'étape suivante ; par exemple, un seul nœud de données peut être mis hors service à la fois. Le Namenode et le secondaryNamenode ne peuvent pas être désactivés ensemble ; il faut également vérifier l'intégrité du Namenode avant de mettre le disque en service.

Figure 474: Vérifications préalables du remplacement de disques



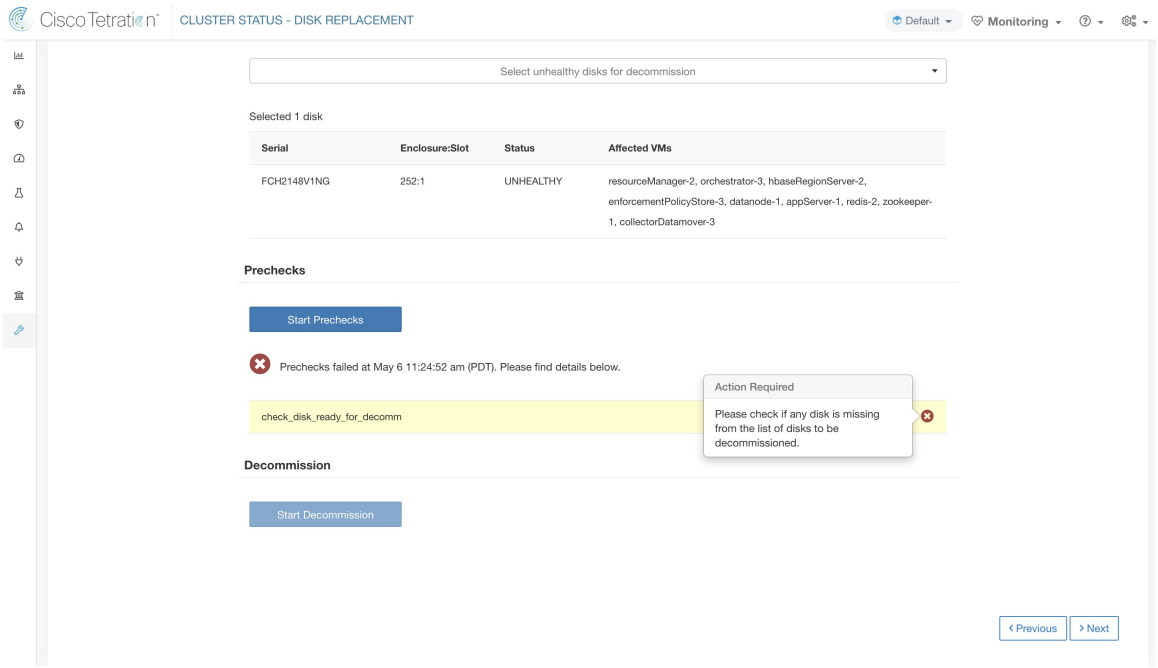
Vous pouvez sélectionner n'importe quel ensemble de disques défaillants à mettre hors service ensemble et lancer les contrôles préalables à la désactivation. La modification de l’ensemble des disques défaillants nécessite une réexécution des vérifications préalables. Effectuez à nouveau les vérification préalables avant de commencer la mise hors service ou la mise en service des disques. Vérifiez qu’il n’y a pas de nouvel échec de vérification préalable entre la dernière exécution de la vérification préalable et le début de la tâche de désactivation.

Figure 475: Disques non intègres pour la désactivation



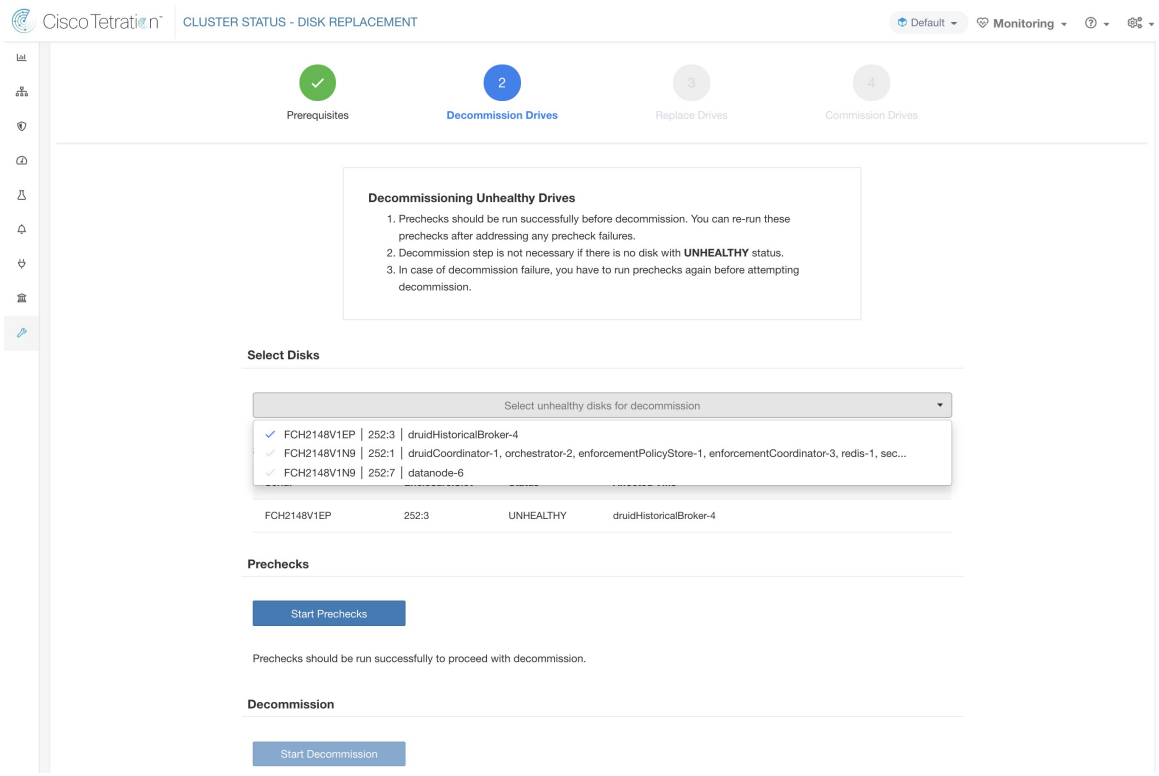
Si une vérification préalable échoue, un message détaillé s'affiche. Cliquez sur le message d'échec; une proposition d'action s'affichera dans une fenêtre contextuelle lorsque le pointeur survolera le bouton en forme de croix.

Figure 476: Action suggérée en cas d'échec de la vérification préalable



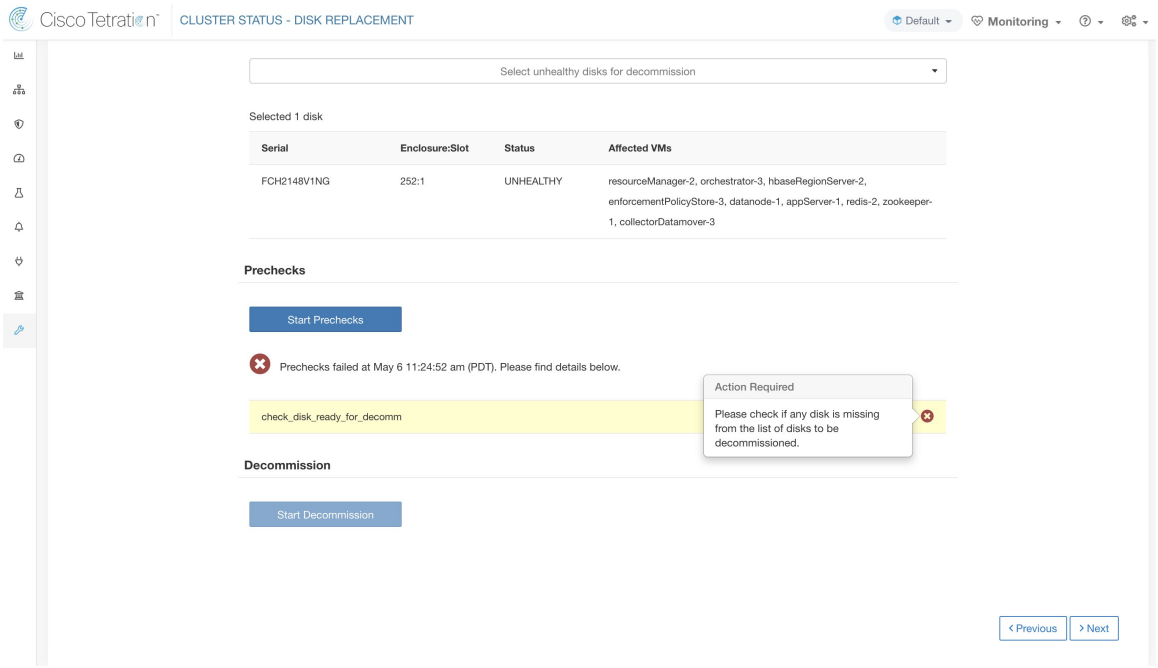
Vous pouvez sélectionner n'importe quel ensemble de disques défaillants à mettre hors service simultanément et lancer la vérification préalable de la mise hors service. La modification de l'ensemble de disques défaillants nécessitera une réexécution de la vérification préalable. Les mêmes vérification préalables sont effectuées à nouveau avant le début de la tâche (mise hors service ou en service) pour s'assurer qu'il n'y a pas de nouvelle défaillance entre la dernière vérification préalable et le début de la tâche de mise hors service.

Figure 477: Sélectionnez les disques NON INTÈGRES à mettre hors service



Après l'échec d'une vérification préalable, un message détaillé s'affiche en cliquant sur le message d'échec, de même qu'une proposition d'action s'affiche dans une fenêtre contextuelle lorsque le pointeur survole le bouton en forme de croix rouge.

Figure 478: Action suggérée dans l'écran contextuel en cas d'échec de la vérification préalable



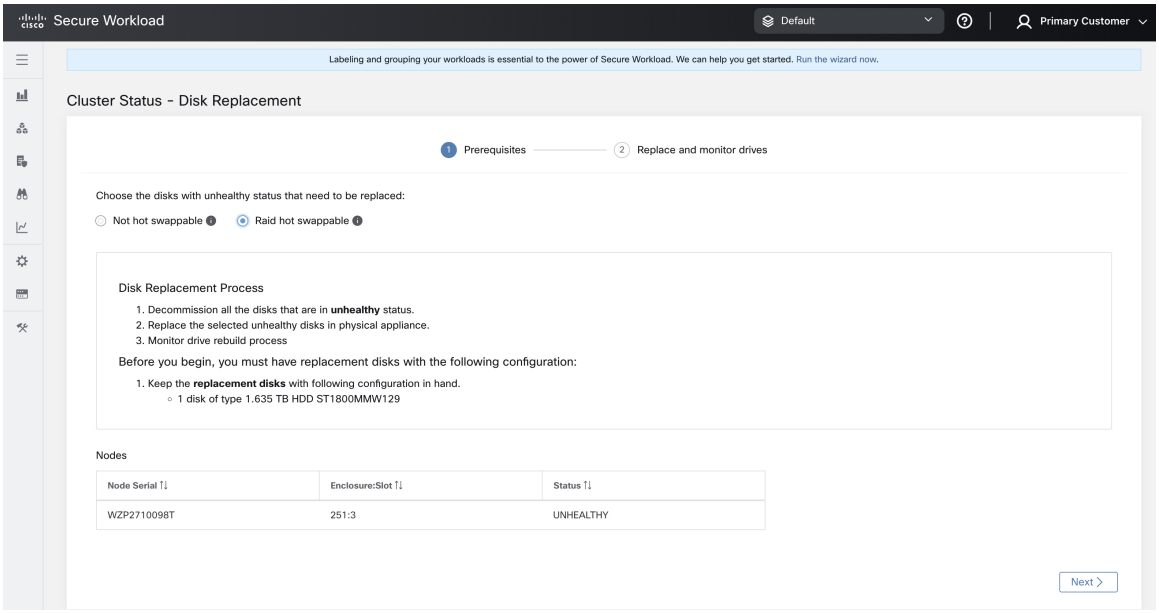
Assistant de remplacement de disques RAID échangeables à chaud

Avant de commencer

Avant de démarrer le processus de remplacement des disques non intègres, assurez-vous que les nouveaux disques sont disponibles.

L' **assistant de remplacement des disques** affiche les détails des disques défaillants, y compris la taille, le type, la marque et le modèle de chaque disque à remplacer. En outre, vous pouvez également afficher l'ID du logement et la liste de toutes les machines virtuelles qui utilisent chacun de ces disques.

Figure 479: Assistant de remplacement de disque



Physiquement, les lecteurs et le matériel sont échangeables à chaud. Cependant, seules les grappes 39RU-G3 (M6) possèdent la configuration matérielle requise pour permettre l'échange d'un lecteur. Une fois le lecteur remplacé, vous pouvez en échanger un sans mettre hors service les machines virtuelles qui utilisent le lecteur avant de pouvoir mettre en service les machines virtuelles sur les grappes.

Si un lecteur s'affiche sous « Non échangeable à chaud », vous devez suivre le processus de « remplacement d'un seul lecteur » pour remplacer ce dernier. Sinon, si un lecteur s'affiche sous « Raid échangeable à chaud », vous pouvez remplacer le lecteur sans désactiver aucune machine virtuelle, car le nœud utilise RAID5 basé sur le matériel.

Note Dans une grappe 39RU M6, les lecteurs compatibles avec RAID sont disponibles sur les nœuds de disque dur. Vous pouvez remplacer les disques RAID échangeables à chaud sans éteindre le système ni perturber son fonctionnement.

Dans une grappe 39RU M6, pour les disques non RAID, vous ne pouvez pas remplacer les disques pendant que le système est en marche. Vous devez éteindre le système avant de remplacer les disques.

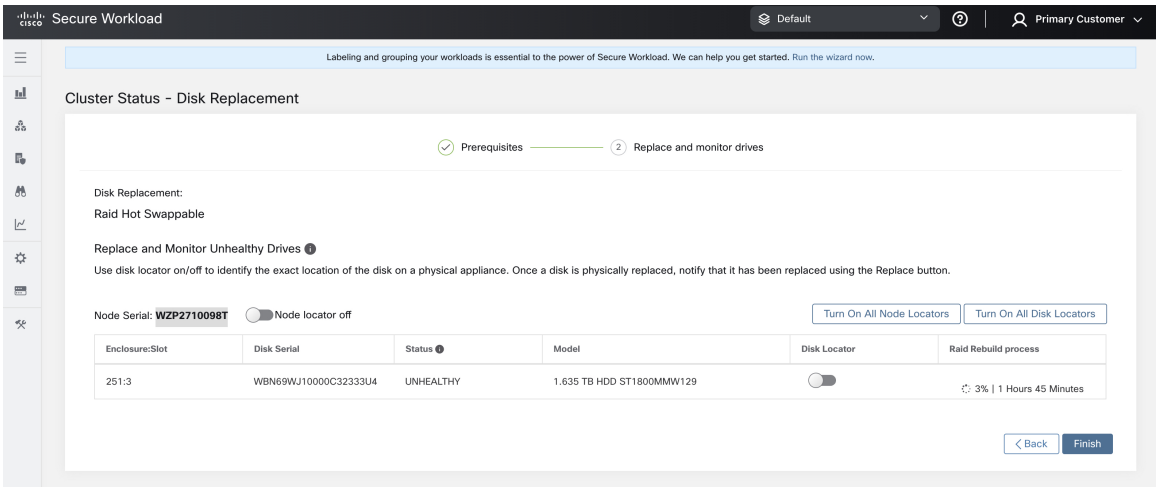
Transition d'état du disque

Dans n'importe quelle grappe pour disques RAID échangeables à chaud, les disques durs ont trois états : **HEALTHY** (INTÈGRE) , **UNHEALTHY** (NON INTÈGRE), et **NEW** (NOUVEAU). Un lecteur **UNHEALTHY** (NON INTÈGRE) passe à un état **HEALTHY** (INTÈGRE), vous pouvez le remplacer une fois que le contrôleur de stockage a terminé le processus de reconstruction de la matrice RAID.

Remplacer des disques RAID échangeables à chaud

Après la désactivation des disques, retirez-les et remplacez-les par de nouveaux. Pour faciliter ce processus, nous avons ajouté un accès repéré par un voyant DEL du localisateur de disque et du serveur sur la page de remplacement. Veillez à éteindre les voyants DEL du serveur et du localisateur de disques.

Figure 480: Reconfigurer les disques nouvellement ajoutés



Les disques peuvent être remplacés physiquement dans n'importe quel ordre, mais ils doivent être reconfigurés dans les numéros d'emplacement du plus petit au plus grand pour un serveur donné. Cet ordre est appliqué sur l'interface utilisateur et le serveur principal (backend). Sur l'interface utilisateur, vous aurez un bouton de remplacement actif pour le disque avec le numéro de logement le plus bas et l'état UNUSED.

Lorsque tous les disques sont remplacés, procédez à la mise en service. Comme pour la désactivation, nous devons exécuter un ensemble de vérification préalables avant de pouvoir poursuivre la mise en service. La progression de la mise en service est surveillée sur la page de mise en service du disque. Une fois la mise en service réussie, l'état de tous les disques passe à HEALTHY (INTÈGRE).

Figure 481: Avancement de la mise en service

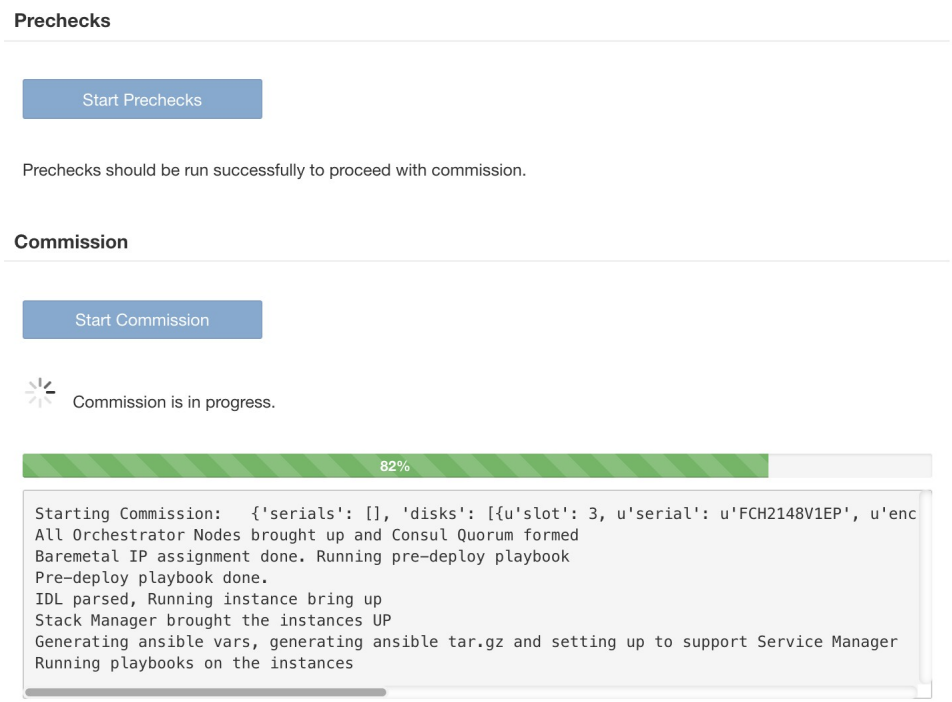
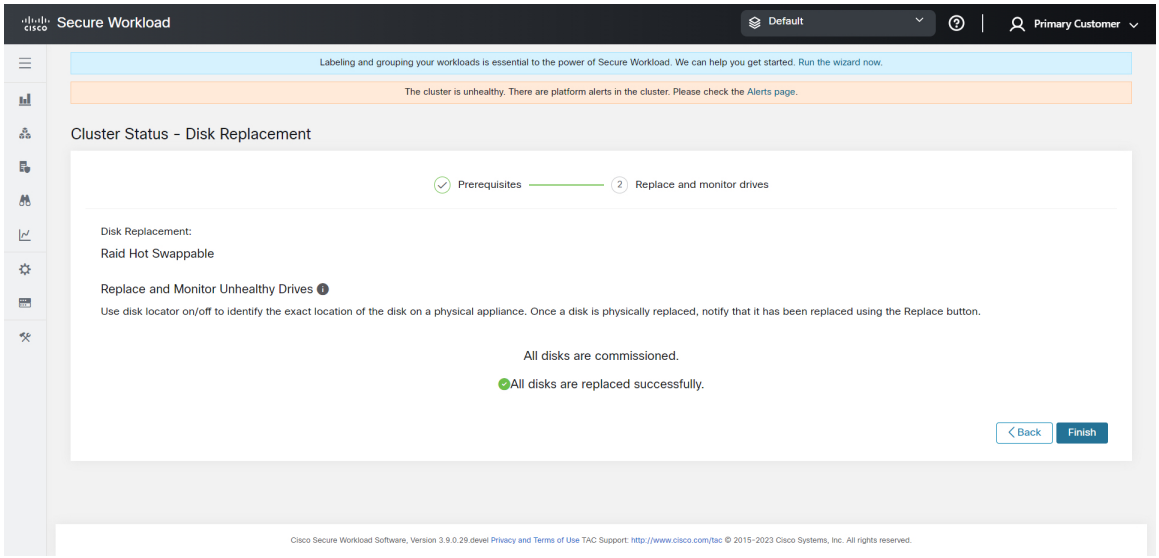


Figure 482: Remplacement du disque



Comportements connus

1. Pour les lecteurs non échangeables à chaud des serveurs, le système d'exploitation de l'hôte est stocké sur le premier lecteur du serveur. Si le premier lecteur (logement 1) du serveur tombe en panne, dans la

plupart des cas, le nœud entier devient inactif et doit être mis hors service, le lecteur doit être remplacé, l'image du serveur est recréée et remise en service dans le système. Contactez l'assistance technique de Cisco pour obtenir de l'aide.

2. Les serveurs RAID échangeables à chaud utilisent un matériel RAID5, qui stocke un bloc de parité pour chaque bloc de données, ce qui permet au système de continuer à fonctionner sans problème tant qu'un seul lecteur est défaillant sur ce serveur. Si plus d'un lecteur tombe en panne sur un serveur doté de lecteurs RAID échangeables à chaud, dans la plupart des cas, le serveur devient inactif et doit être mis hors service, les lecteurs doivent être remplacés, puis le serveur peut être recréé et remis en service dans le système. Contactez l'assistance technique de Cisco pour obtenir de l'aide.
3. Si plusieurs lecteurs non échangeables à chaud tombent en panne sur le même serveur, cliquez sur les boutons **Replace** (remplacer) dans l'interface utilisateur pour passer du numéro de logement le plus bas au numéro de logement le plus élevé sur chaque serveur.
4. Après avoir cliqué sur le bouton **Replace** (Remplacer) pour un lecteur non échangeable à chaud, il faut de 3 à 10 minutes au lecteur pour passer de REPLACED (REMPLACÉ) à NEW (NOUVEAU) dans l'interface utilisateur.
5. Après le remplacement physique d'un lecteur RAID échangeable à chaud, il faut de 3 à 10 minutes avant que l'état du processus de reconstruction s'affiche dans l'interface utilisateur.
6. Une grappe 39RU-G3 déployée à l'aide de Cisco Secure Workload version 3.8 ne sera pas configurée avec des disques RAID échangeables à chaud. La grappe devra être redéployée à l'aide de Cisco Secure Workload version 3.9, ou chaque TA-BNODE-G3 et TA-CNODE-G3 devra être mis hors service, recréé et remis en service un à la fois après la mise à niveau de la grappe vers la version Cisco Secure Workload 3.9. Si la méthode de désactivation, de recréation ou de mise en service de conversion de TA-BNODE-G3 et de TA-CNODE-G3 en disques RAID échangeables à chaud est utilisée, vérifiez que l'état du service de grappe est vert pour tous les services avant de commencer la désactivation.

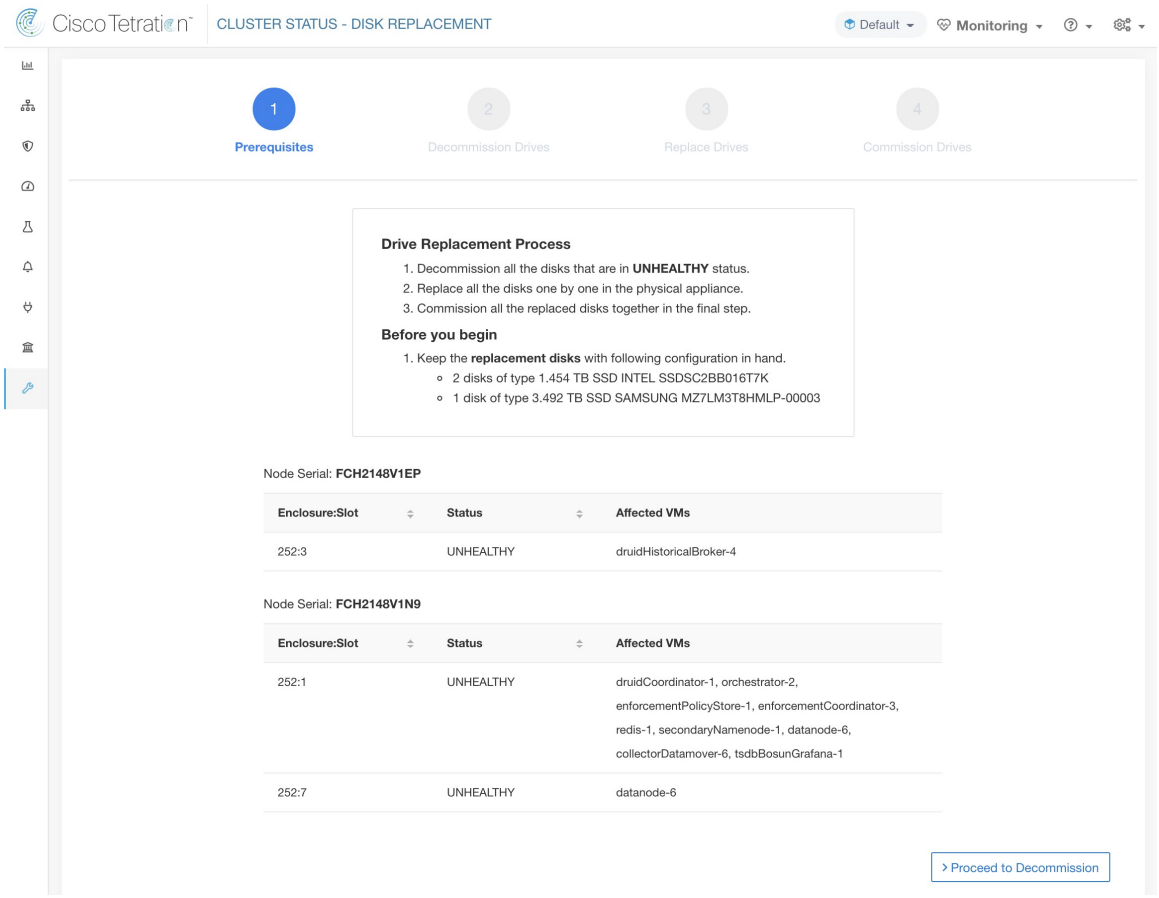
Assistant de remplacement de disque, non échangeable à chaud

Avant de commencer

Avant de commencer le processus de remplacement des disques non intègres, assurez-vous que les nouveaux disques sont disponibles.

L' **assistant de remplacement de disques** affiche les détails des disques défaillants, y compris la taille, le type, la marque et le modèle de chaque disque à remplacer. En outre, vous pouvez également afficher l'ID de logement et les listes de toutes les machines virtuelles qui utilisent chacun de ces disques.

Figure 483: Assistant de remplacement de disque



Note Physiquement, les lecteurs et le matériel sont échangeables à chaud.

Transitions d'état de disque

Dans une grappe, pour un système non-RAID, il y a six états pour les disques durs ;**HEALTHY** (INTÈGRE), **UNHEALTHY** (NON INTÈGRE), **UNUSED** (INUTILISÉ, **REPLACED** (REMPLACÉ), **NEW** (NOUVEAU), et **INITIALIZED** (INITIALISÉ). Après le déploiement ou la mise à niveau de la grappe, l'état de chaque disque de la grappe est **HEALTHY**. L'état d'un ou de plusieurs disques peut devenir **UNHEALTHY** en fonction de la détection de diverses erreurs.

Note Les disques non échangeables à chaud sont disponibles uniquement pour les grappes M4 et M5.

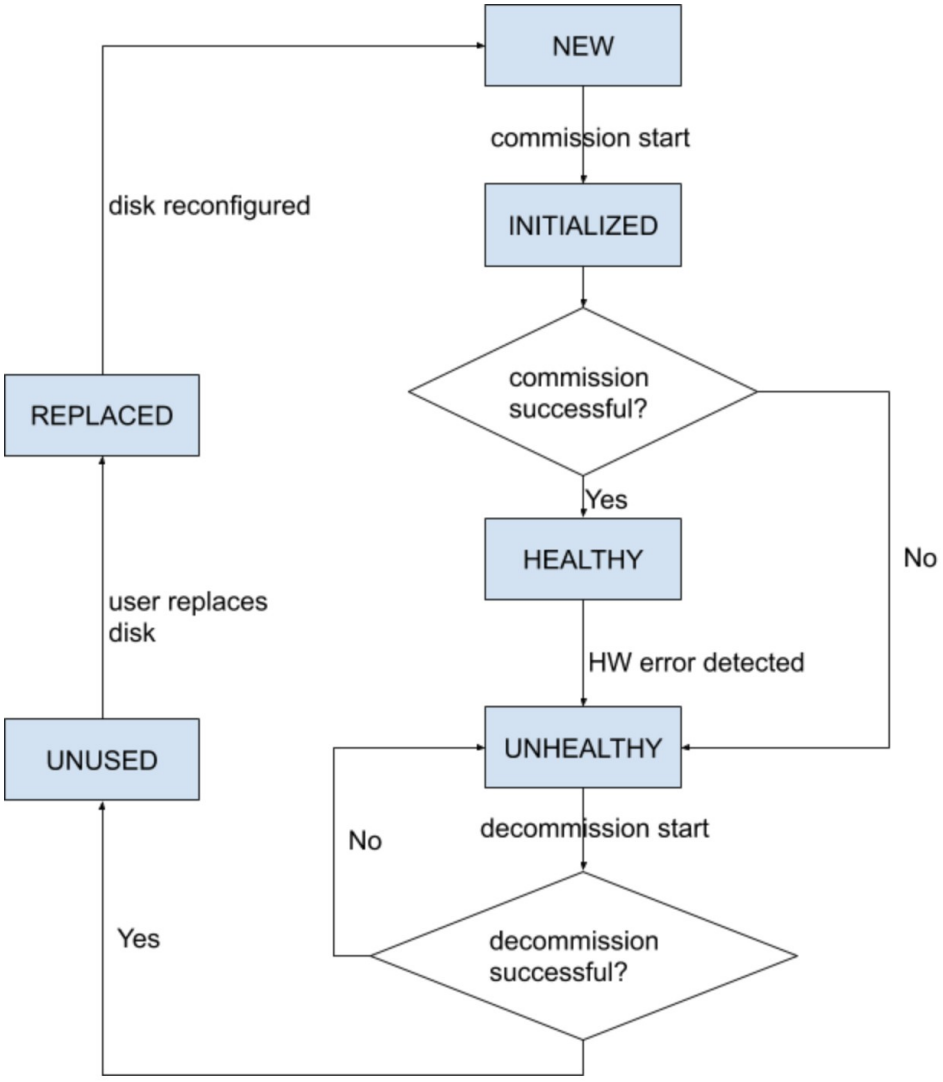
Aucune action n'est entreprise, sauf si l'état d'un disque passe à **UNHEALTHY**. Avant de commencer la mise en service des disques, déployez toutes les machines virtuelles qui ont été supprimées dans le cadre du processus de désactivation.

Une fois que vous avez mis en service les disques sans erreur, l'état des disques passe à **HEALTHY**. Dans le cas où la mise en service du disque échoue, l'état affiche **UNHEALTHY**. Pour les disques qui sont à l'état **UNHEALTHY**, démarrez le processus de désactivation du disque. Si le processus de désactivation réussit, l'état du disque passe à **UNUSED**, et si les disques tombent en panne lors de la désactivation, répétez le processus jusqu'à ce que l'état des disques devienne **UNUSED**.

Retirez les disques **UNHEALTHY** de la grappe et remplacez-les par de nouveaux disques, l'état devient **REPLACED).** Reconfigurer les disques de remplacement et analyser le matériel à la recherche d'anomalies. Si aucune anomalie n'est détectée, l'état des disques devient **NEW**, sinon vous devrez peut-être résoudre le problème; La modification d'état peut prendre jusqu'à trois minutes.

Pour comprendre comment les modifications d'état du disque sont gérées, consultez l'ordinogramme ci-dessous :

Figure 484: Transitions d'état de disque



Désactiver le disque

Une fois les vérifications préalables effectuées, vous pouvez procéder à la désactivation du disque. La progression de la désactivation sera affichée lors de l'assistant de remplacement du disque. Lorsque la progression de la désactivation atteint 100 %, l'état de tous les disques mis hors service devient UNUSED (INUTILISÉ).

Figure 485: Surveiller la progression de la désactivation des disques

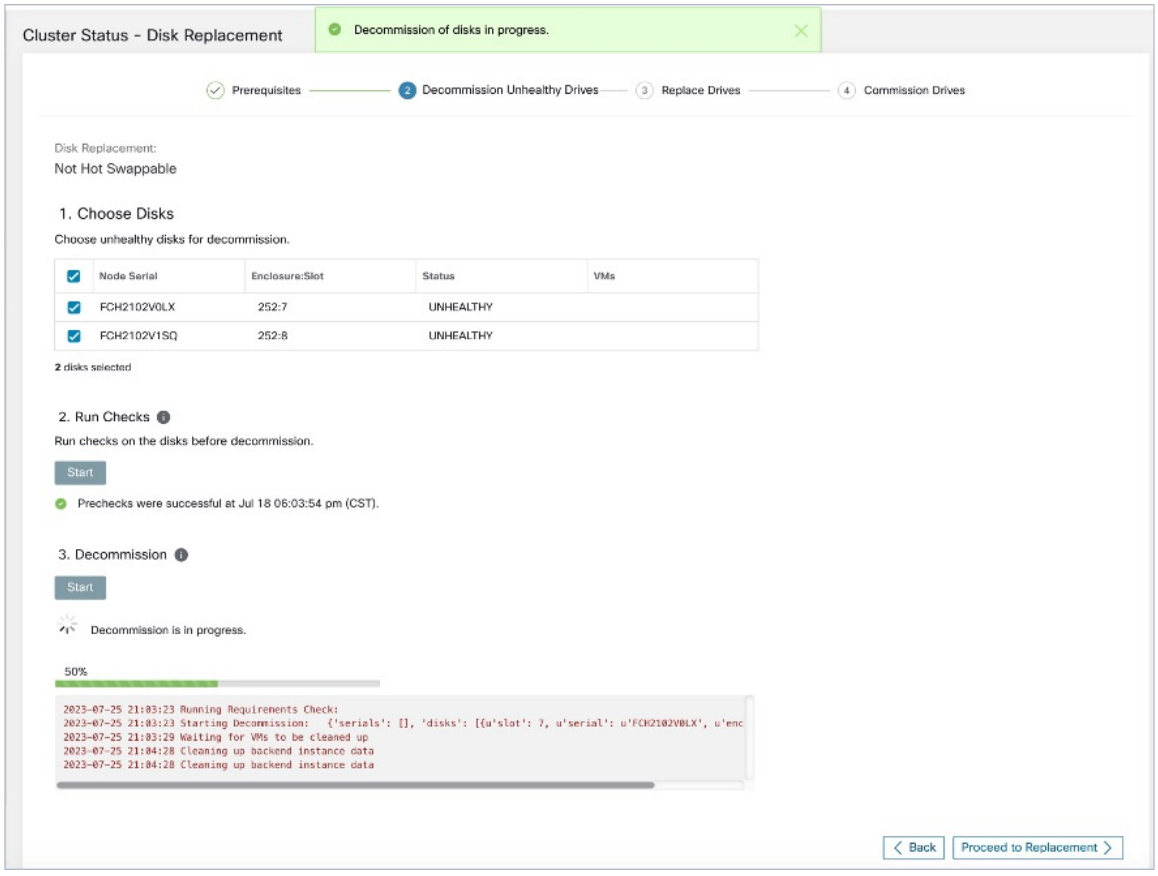
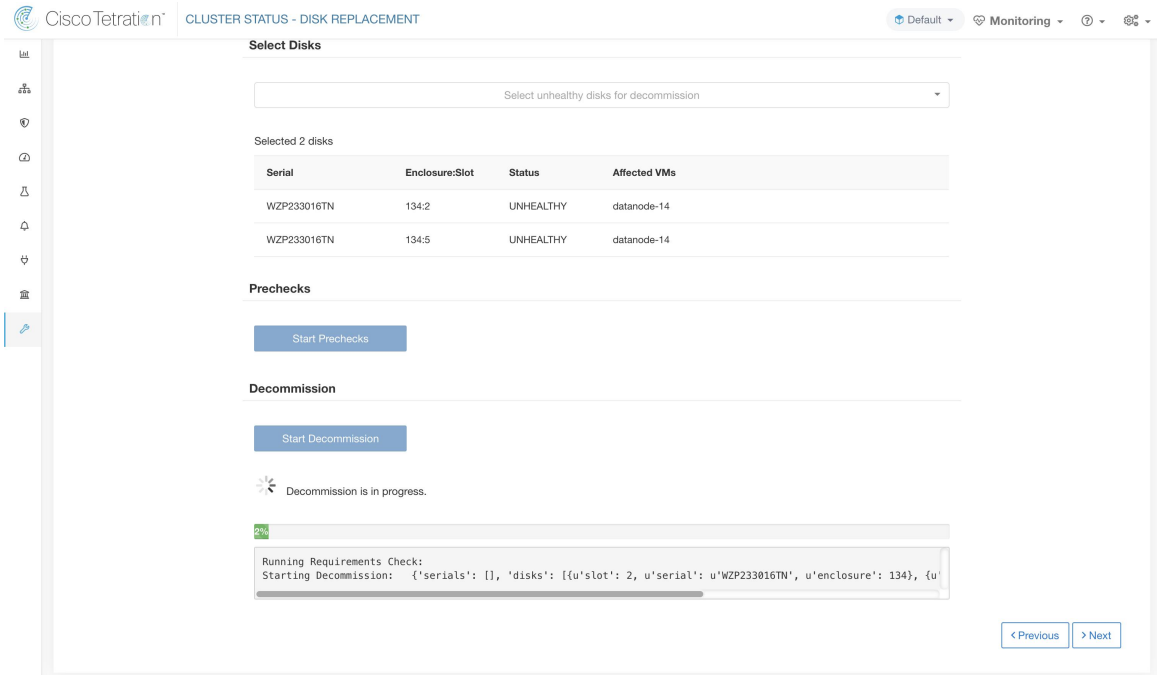


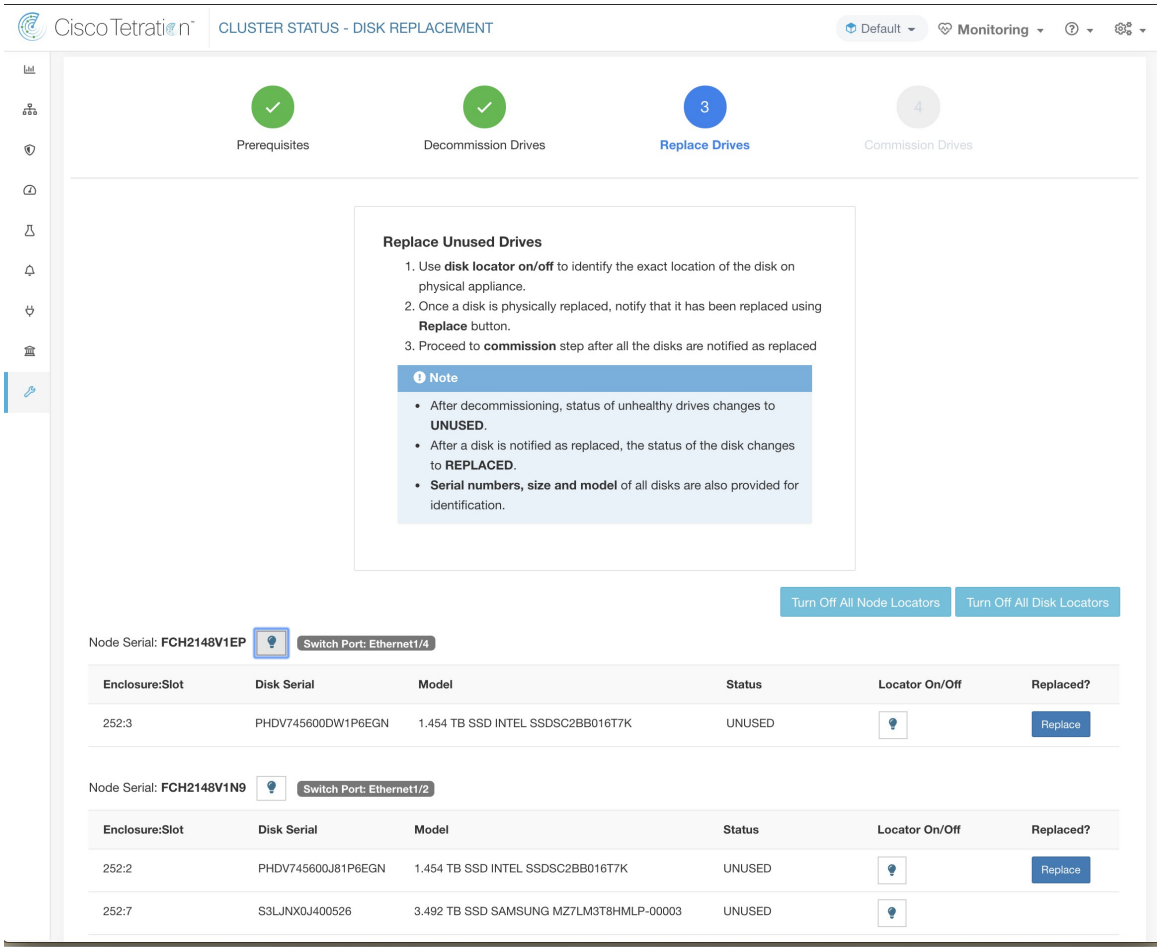
Figure 486: Surveiller la progression de la désactivation des disques



Remplacer le disque

Après la désactivation des disques, retirez-les et remplacez-les par de nouveaux. Pour faciliter ce processus, nous avons ajouté un accès repéré par un voyant DEL du localisateur de disque et du serveur sur la page de remplacement. Veillez à éteindre les voyants DEL du serveur et du localisateur de disques.

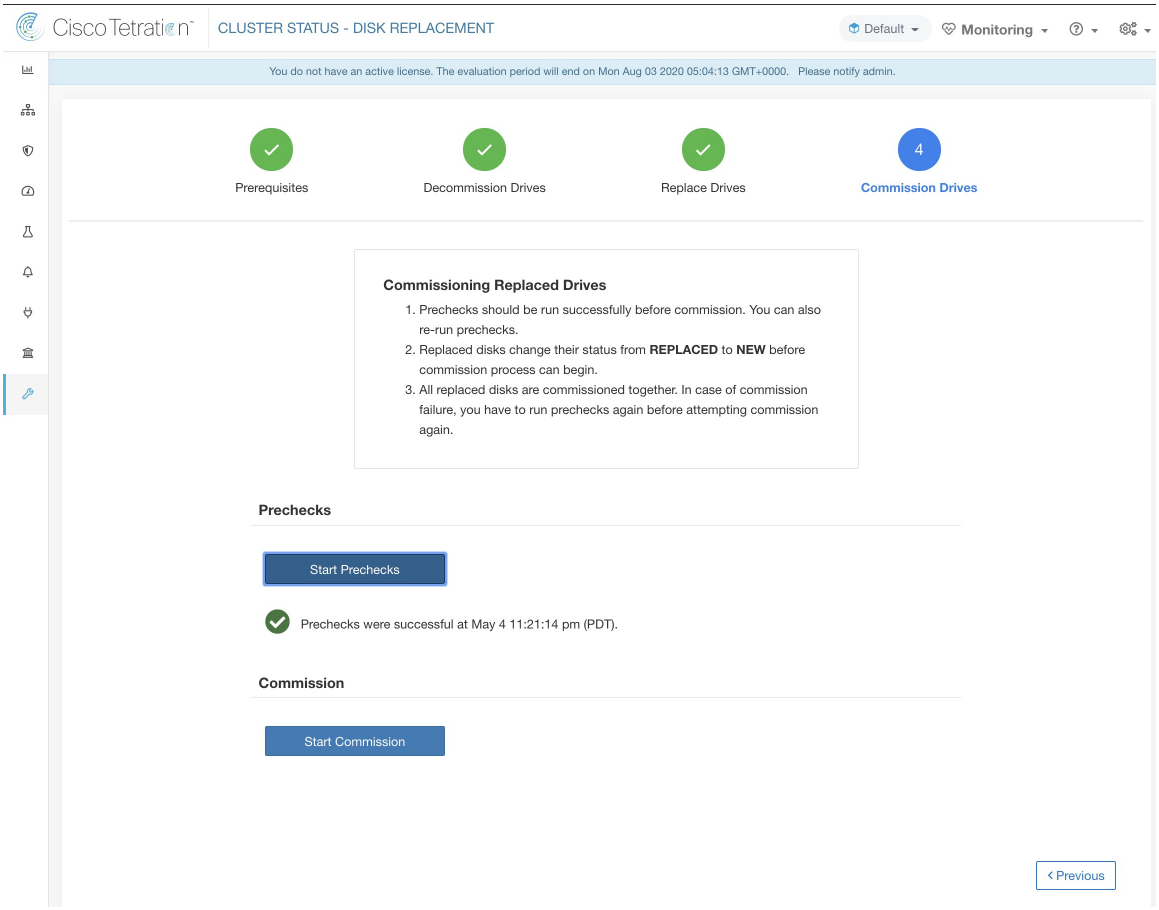
Figure 487: Reconfigurer les disques nouvellement ajoutés (non échangeables à chaud)



Les disques peuvent être remplacés physiquement dans n'importe quel ordre, mais ils doivent être reconfigurés dans les numéros d'emplacement du plus petit au plus grand pour un serveur donné. Cet ordre est appliqué sur l'interface utilisateur et le serveur principal (backend). Sur l'interface utilisateur, vous aurez un bouton de remplacement actif pour le disque avec le numéro de logement le plus bas et l'état UNUSED.

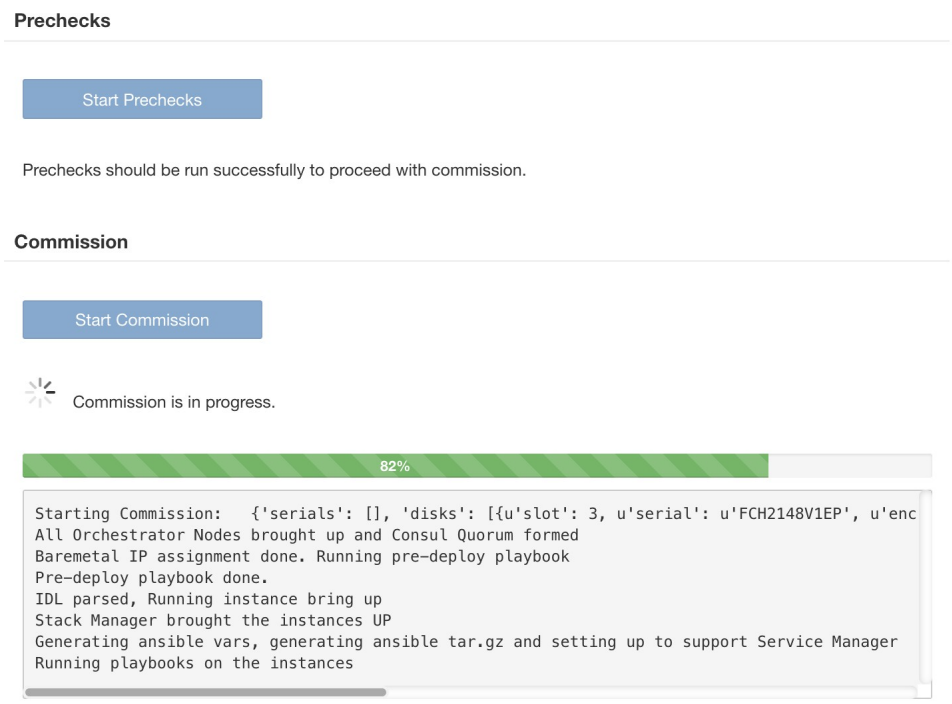
Mettre à disposition le disque

Lorsque tous les disques sont remplacés, procédez à la mise en service. Comme pour la désactivation, nous devons exécuter un ensemble de vérification préalables avant de pouvoir poursuivre la mise en service.



La progression de la mise en service est surveillée sur la page de mise en service du disque. Une fois la mise en service réussie, l'état de tous les disques passe à HEALTHY (INTÈGRE).

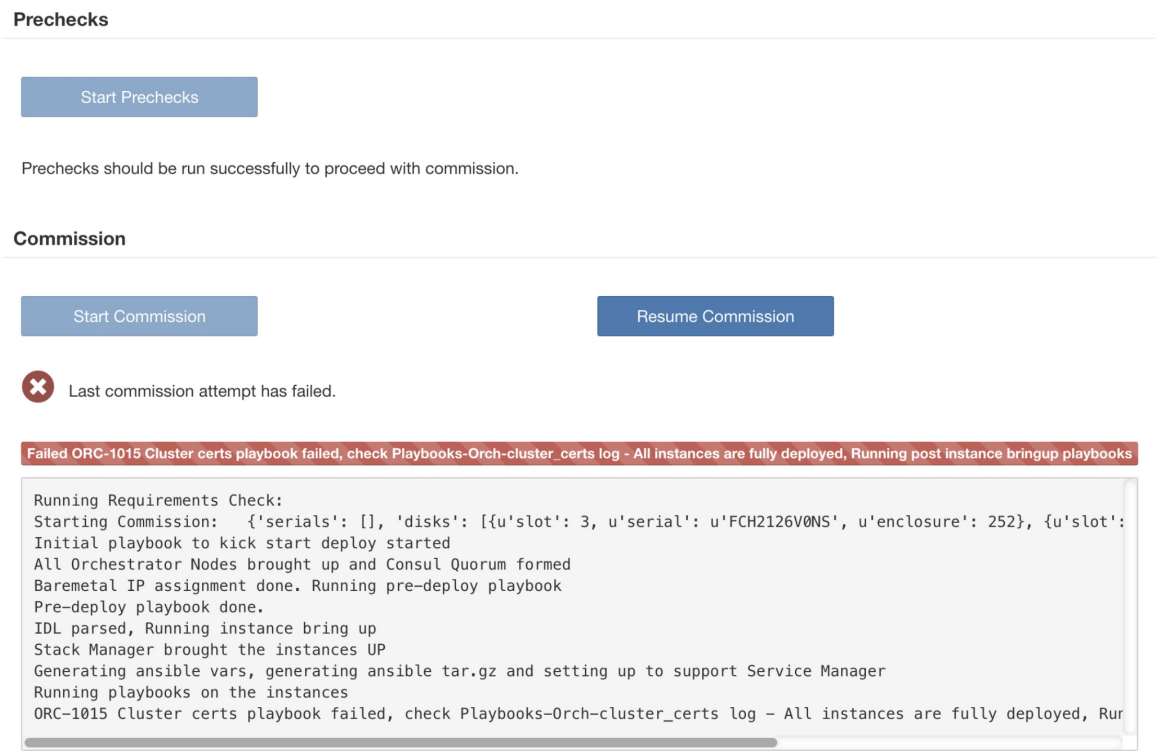
Figure 488: Avancement de la mise en service



Reprise sur échec pendant la mise en service du disque

Après avoir déployé les machines virtuelles et en cas de défaillance, vous pouvez les restaurer à l'aide du bouton**Resume Commission** (Reprendre la mise en service). Pour poursuivre la mise en service du disque, cliquez sur le bouton **Resume Commission** (Reprendre a mise e service) pour redémarrer les guides post-déploiement.

Figure 489: Reprendre la mise en service



En cas de défaillance avant le déploiement des machines virtuelles, les disques mis en service précédemment verront leur état passer à UNHEALTHY (NON INTÈGRE). Cela nous obligera à redémarrer le processus de remplacement à partir de la désactivation des disques UNHEALTHY (NON INTÈGRE).

Défaillance de disque pendant la mise en service

En cas de défaillance d'un disque autre que ceux qui sont remplacés alors que la mise en service du disque est en cours, l'assistant de remplacement de disque affichera une notification de cette défaillance à la fin du processus de mise en service en cours, qu'il ait réussi ou échoué.

En cas d'échec avec reprise, les utilisateurs ont deux possibilités quant aux prochaines étapes à effectuer.

1. Ils peuvent essayer de reprendre et de terminer la mise en service en cours et effectuer ultérieurement le processus de remplacement du disque en ce qui concerne les nouvelles défaillances.
2. Ils peuvent également commencer à mettre hors service le nouveau disque défectueux et procéder à la mise en service de tous les disques simultanément.

Cette deuxième possibilité est la seule disponible en cas de défaillance ne pouvant pas être reprise. Si l'échec post-déploiement est causé en raison des nouveaux disques défaillants, la deuxième possibilité sera à nouveau la seule voie à suivre, bien qu'un bouton de reprise soit disponible.

Problèmes connus et dépannage

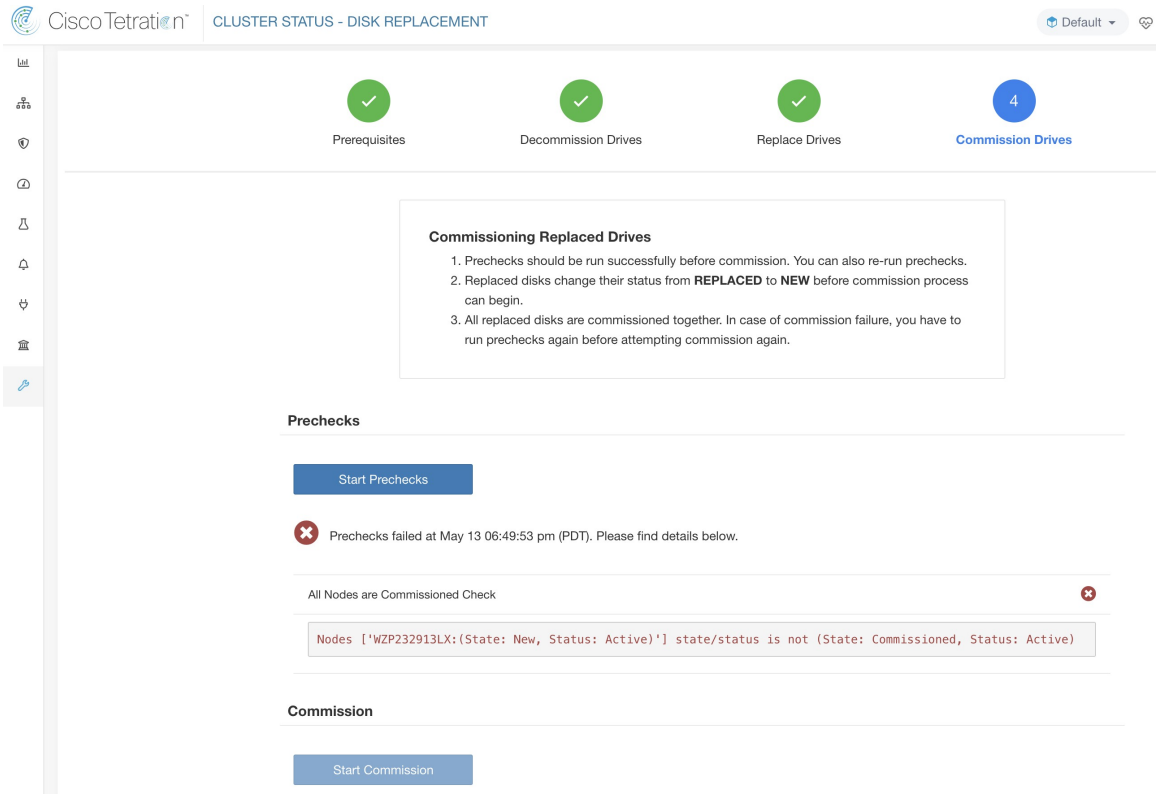
- Le disque contenant les volumes racine du serveur ne peut pas être remplacé à l'aide de cette procédure. De telles défaillances de disques doivent être corrigées à l'aide du processus de maintenance du serveur.

- La mise en service du disque ne peut avoir lieu que lorsque tous les serveurs sont actifs et en état de mise en service. Consultez la section *Special Handling* (manutention spéciale) qui décrit comment procéder dans les cas où une combinaison de remplacement du disque et du serveur est nécessaire.
- Les disques SSD sont trop chers et ont un taux de défaillance très faible. Nous ne voulons donc pas perdre une capacité précieuse pour le stockage de données redondantes.
- Sur les grappes M6 déployées à l'origine avec le logiciel 3.8, lorsqu'un serveur est mis en service avec le logiciel 3.9, la configuration RAID sera appliquée aux disques durs. Ainsi, une grappe contiendra certains nœuds avec la configuration de disques RAID et d'autres non RAID dans la version 3.8. Il est probable que votre matériel Cisco Secure Workload 39RU ait été livré à l'origine avec la version 3.9 déjà installée, mais certains des premiers M6 ont été livrés avec la version 3.8 déployée.
- Vous pouvez convertir une grappe au format RAID si la désactivation et la mise en service du serveur sont effectuées progressivement sur tous les serveurs après mise à niveau vers la version 3.9 du logiciel.
- Les grappes M6 8RU sont uniquement des nœuds SSD et RAID n'est pas configuré sur les disques SSD. Par conséquent, les 8RU ne disposent pas de RAID.
- La configuration de disques sur des générations antérieures (M4/M5) nous empêche de prendre en charge RAID sur ces générations de matériel Cisco Secure Workload.

Remplacements des disques et des serveurs

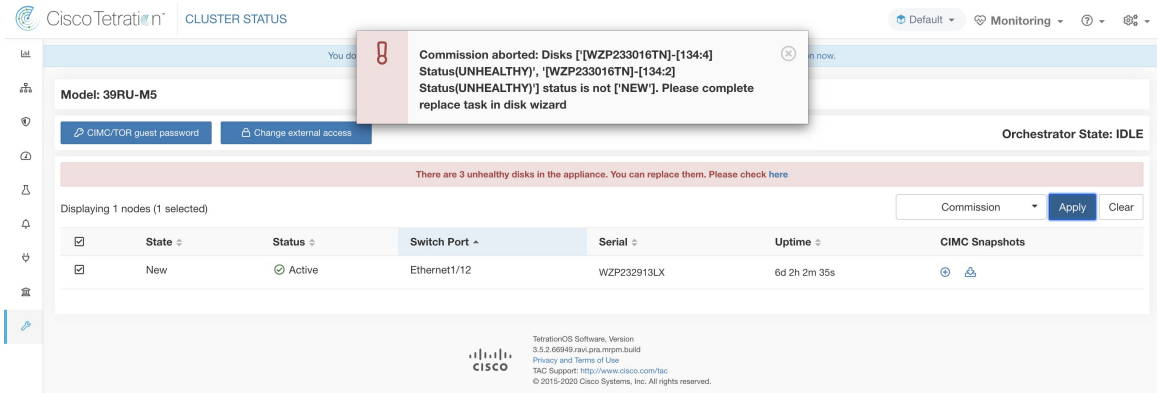
Dans le cas des scénarios de défaillance dans lesquels un disque et un serveur doivent être mis en service simultanément, l'utilisateur est censé mettre hors service et remplacer tous les disques qui peuvent être mis hors service. La mise en service de ces disques serait empêchée par la vérification préalable qui assure que

1. Tous les disques non intègres sont à l'état NEW (NOUVEAU)
2. Tous les serveurs sont dans l'état *commissioned* (mis en service) avec l'état *active* (actif)



Une fois que tous les disques UNHEALTHY (NON INTÈGRE) sont à l'état NEW (NOUVEAU), le serveur défaillant doit être mis hors service/recréé dans l'image/remis en service à l'aide de la procédure d'entretien du serveur.

Désormais, la mise en service du serveur sera bloquée si un disque n'est pas dans l'état HEALTHY (INTÈGRE) ou NEW (NOUVEAU). Une mise en service réussie du serveur aura également pour effet de rendre l'état de tous les disques HEALTHY (INTÈGRE)



Opérations d'entretien de la grappe

Cette section décrit les opérations d'entretien qui affectent l'ensemble de la grappe.

Arrêter la grappe Cisco Secure Workload

L'arrêt de la grappe arrête tous les processus Cisco Secure Workload en cours et met hors tension tous les nœuds. Effectuez les étapes suivantes pour arrêter la grappe.

Lancer l'arrêt de la grappe

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)** .

Étape 2 Cliquez sur l'onglet **Reboot/Shutdown** (Redémarrage/arrêt).

Étape 3 Sélectionnez **Shutdown** (Arrêt) et cliquez sur **Send Shutdown Link** (Envoyer un lien d'arrêt). Le lien d'arrêt est envoyé à l'adresse courriel .

Figure 490: Adresse courriel relative à l'arrêt

Hello Site Admin!

We received a request that you intend to shutdown the cluster "98". You can do this through the link below.

Shutdown 98 (For best results, please use Google Chrome)

The above link expires by Jul 22 08:34:30 pm (PDT).

If you didn't request this, please ignore this email.

Shutdown will not be triggered until you actually click the above link.

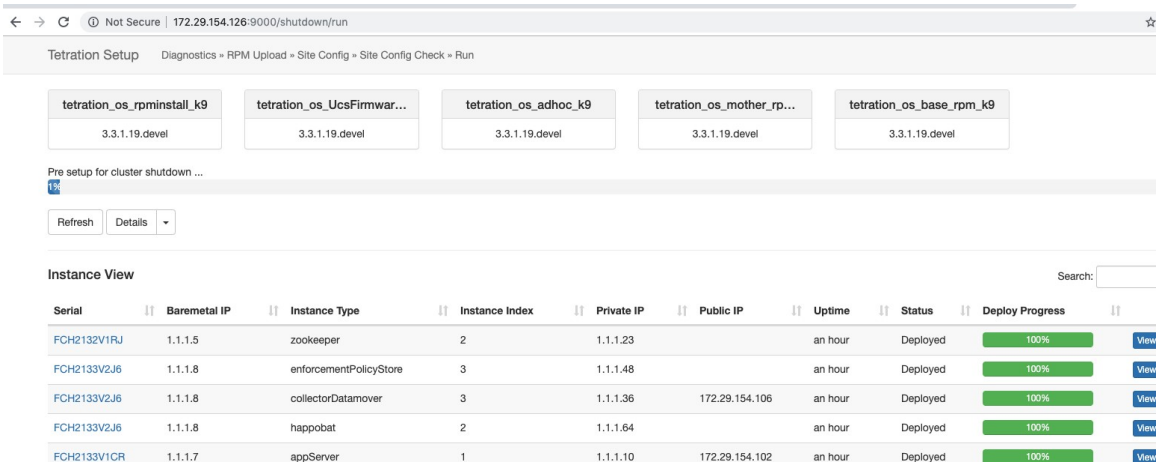
Étape 4 Dans la page **Cluster Shutdown** (arrêt de la grappe), cliquez sur **Shutdown** (Arrêt).

Important Vous ne pouvez pas annuler l'arrêt après avoir cliqué sur le bouton **Shutdown** (Arrêt).

Progression de l'arrêt de la grappe

Après avoir lancé l'arrêt de la grappe, la progression de l'arrêt et l'état sont affichés.

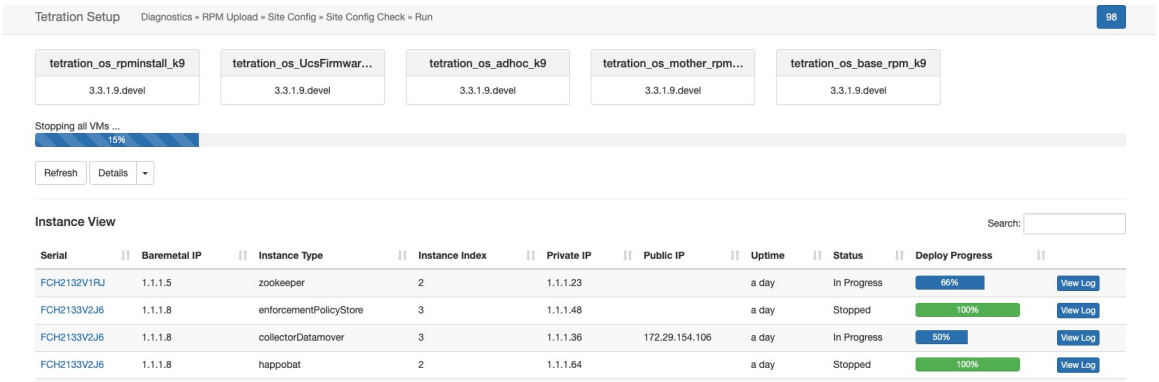
Figure 491: Progression de l'arrêt de la grappe



Si une erreur se produit lors des vérifications préalables à l'arrêt initiales, la barre de progression devient rouge. Vous devez alors cliquer sur le bouton de reprise pour redémarrer l'arrêt après avoir corrigé les erreurs.

Une fois les vérification préalables terminées, les machines virtuelles sont arrêtées. Au fur et à mesure que les machines virtuelles s'arrêtent, la progression s'affiche. La page est similaire à l'arrêt de la machine virtuelle en cas de mises à niveau. Pour en savoir plus, reportez-vous à la section relative aux mises à niveau de chaque champ. L'arrêt de toutes les machines virtuelles peut prendre jusqu'à 30 minutes.

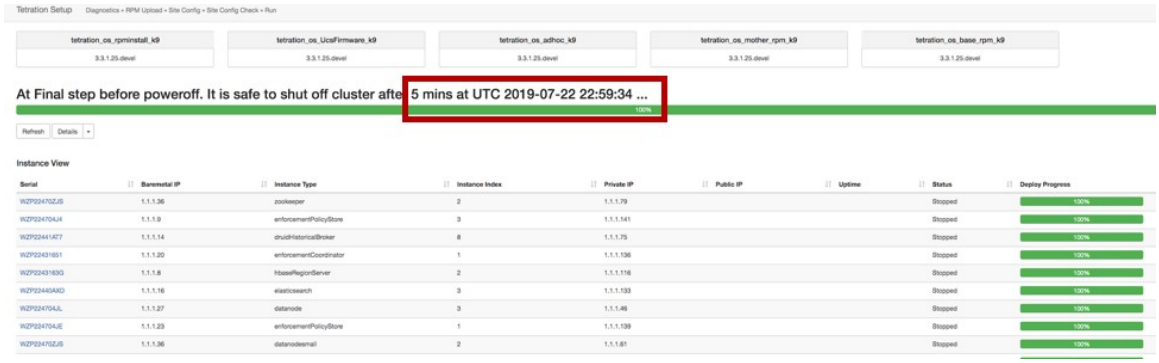
Figure 492: Arrêter les VM



Lorsque la grappe est prête à être arrêtée, la barre de progression passe à 100 % et indique le délai après lequel il est possible d'éteindre la grappe en toute sécurité. Consultez la mise en évidence dans la capture d'écran suivante.

Note Ne mettez pas la grappe hors tension avant d'avoir attendu que l'heure s'affiche dans la barre de progression.

Figure 493: Arrêt à 100 %



Redémarrer la grappe Cisco Secure Workload

Pour récupérer la grappe après l'arrêt, mettez sous tension les éléments sans système d'exploitation. Lorsque tous les éléments sans système d'exploitation sont opérationnels, l'interface utilisateur devient accessible. Après vous être connecté à la grappe, redémarrez-la pour la rendre opérationnelle.

Note Vous *devez* redémarrer la grappe après un arrêt pour la rendre opérationnelle.

Initier le redémarrage de la grappe

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)** .

Étape 2 Cliquez sur l'onglet **Reboot/Shutdown** (Redémarrage/arrêt).

Étape 3 Sélectionnez **Reboot** (Redémarrer) et cliquez sur **Send Reboot Link**(Envoyer le lien de redémarrage).

Cliquez sur le lien que vous recevez sur votre identifiant de courriel pour redémarrer la grappe. Dans la page de configuration de l'interface utilisateur, lancez le redémarrage de la grappe. Pendant le redémarrage, une opération de mise à niveau restreinte est effectuée.

Afficher l'historique des tâches d'entretien de la grappe

Pour afficher les tâches d'entretien de la grappe précédemment exécutées :

1. Accédez à **Platform(Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**, puis cliquez sur l'onglet **History** (Historique).

   La colonne des opérations de grappe répertorie les tâches telles que le déploiement, la mise à niveau, le redémarrage ou l'arrêt.

2. Pour télécharger les journaux des tâches de grappe, cliquez sur **Download Logs** (Télécharger les journaux).

Reset the Secure Workload Cluster

Caution

- The cluster reset process is irreversible. All the data stores within the cluster are cleared.
- During the reset, information about the previous state of the cluster is not saved.
- All the services running on the cluster are stopped.

Note Do not use the **Cluster Reset** option to troubleshoot cluster-related issues. Use the option only when required.

We recommend that you contact Cisco Technical Assistance Center for assistance in resetting the cluster.

The **Reset** option is used to stop all the services and clear all the data stores within the Secure Workload cluster. The reset process takes up to six hours to complete. After the cluster is reset, the services are initialized from the beginning and brought back online.

Note

- The **Cluster Reset** option is applicable to Secure Workload on-premises clusters.
- Both the primary and the secondary clusters can be reset.
- *The **Cluster Reset** option can also be used to switch the cluster mode from active to standby (to configure the primary cluster as the secondary cluster.)*
- Only site admins can reset clusters.

Procedure

Étape 1 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Étape 2 Click **Reset** and perform the following actions:

a) Import and verify the SSH key.
b) After the SSH key is verified, select **I acknowledge that the above SSH key is valid**.
c) Select **Reset**.
d) Click **Send Reset Link**.

An email with the IPv4 link and access token is sent to the registered email ID to reset the cluster. The link remains active for six hours. Clicking the link redirects you to the **Cisco Secure Workload Setup** page.

Étape 3 On the **Cisco Secure Workload Setup** page, perform the following actions:

a) Click **Reset**, and to confirm, click **Yes**.

The services are stopped and the data stores within the cluster are deleted. The progress of the activity is displayed and it takes around 10 minutes to complete.

Caution During the cluster reset process, the Secure Workload GUI and Secure Workload Setup page are not available for 20 to 30 minutes.

After the process is completed, the **Site Config** page is displayed. The required RPMs that have to deploy the cluster are automatically uploaded and the corresponding site configurations configured.

Note You are automatically redirected to the **Site Config** page. The following steps will not work if you try to access the page before the redirection. If redirection takes time to get completed when RPMs and backup data are being uploaded, contact Cisco Technical Assistance Center.

b) To change the cluster mode to **Standby**, click the **Standby Config** toggle button.
c) Enter the primary cluster site name and FQDNs.
d) Click **Continue**.

Note On the **Deploy** page, if you click **Reset Deployment** during the cluster reset operation, then the external IP address is cleared and all the site information must be configured. The **Secure Workload Setup** page can be accessed only on 2.2.2.2.

After 4 to 5 hours, the Secure Workload cluster is deployed and the services are brought back online.

Note If the primary cluster is reset, you must reconfigure all the required software agents, secure connector, connectors, external orchestrators, and other configurations.

Known Issues During Secure Workload Cluster Reset

Note The Secure Workload UI is not available during Cluster Reset. Any failure after the UI becomes inaccessible cannot be resumed. To troubleshoot and deploy the cluster, contact Cisco Technical Assistance Center .

Known Issues

- During the cluster reset operation, the Secure Workload UI and Secure Workload Setup page are not accessible for 20–30 minutes.
- The cluster is reset to the base Secure Workload release version and not to the patch release. Manually upgrade the cluster to the patch release. For more information on upgrading to the patch releases, see Cisco Secure Workload Upgrade Guide.
- You must use the IPv4 link that is provided in the email to reset the cluster; IPv6 link is not supported.
- Only the necessary site configurations are editable during cluster reset, other options cannot be edited.

Administrateur de surveilleur de données : surveilleurs de données

Dérivations de données

Note Cisco Secure Workload prend en charge l'écriture sur Kafka Broker 0.9.x, 10.1.x, 1.0.x et 1.1.x pour les dérivations de données.

Pour envoyer des alertes à partir de la grappe Cisco Secure Workload, vous devez utiliser un surveilleur de données configuré. Les utilisateurs administrateurs surveilleurs de données peuvent configurer et activer des surveilleurs de données nouveaux ou existants. Vous pouvez afficher les dérivations de données de votre **détenteur**.

Figure 494: Dérivations de données disponibles

Pour gérer les surveilleurs de données, dans le volet de navigation, choisissez **Manage (Gestion)** > **Data Tap Admin (Administration des surveilleurs de données)**.

Configuration KafKa recommandée

Lors de la configuration de la grappe Kafka, nous vous recommandons d'utiliser les ports de 9092, 9093 ou 9094, car Cisco Secure Workload ouvre ces ports pour le trafic sortant pour Kafka.

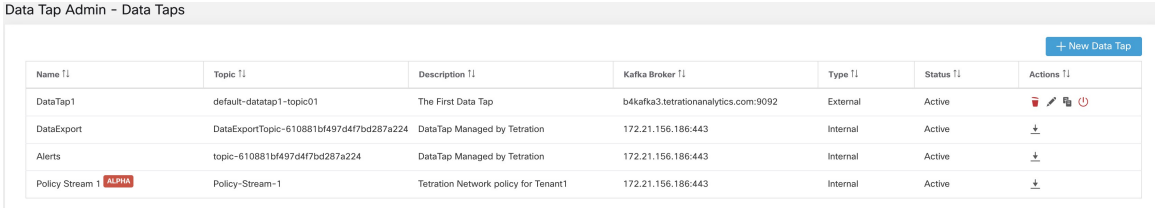
Voici les paramètres recommandés pour les intermédiaires de Kafka :

```
  broker.id=<incremental number based on the size of the cluster>
  auto.create.topics.enable=true
  delete.topic.enable=true
  listeners=PLAINTEXT://:9092
  port=9092
  default.replication.factor=2
  host.name=<your_host_name>
  advertised.host.name=<your_adversited_hostname>
  num.network.threads=12
  num.io.threads=12
  socket.send.buffer.bytes=102400
  socket.receive.buffer.bytes=102400
  socket.request.max.bytes=104857600
  log.dirs=<directory where logs can be written, ensure that there is sufficient space to
hold the kafka journal logs>
  num.partitions=72
  num.recovery.threads.per.data.dir=1
  log.retention.hours=24
  log.segment.bytes=1073741824
  log.retention.check.interval.ms=300000
  log.cleaner.enable=false
  zookeeper.connect=<address of zookeeper ensemble>
  zookeeper.connection.timeout.ms=18000
```

Section d'administration du surveilleurs de données

Les **administrateurs de surveilleurs de données** peuvent afficher les surveilleurs de données disponibles et les configurer en accédant à **Manage(Gestion)** > **Data Tap Admin(Administration des surveilleurs de données)** > **Data Taps (Surveilleurs de données)**. Les dérivations de données sont configurées par **détenteur**.

Figure 495: Toutes les dérivations de données disponibles

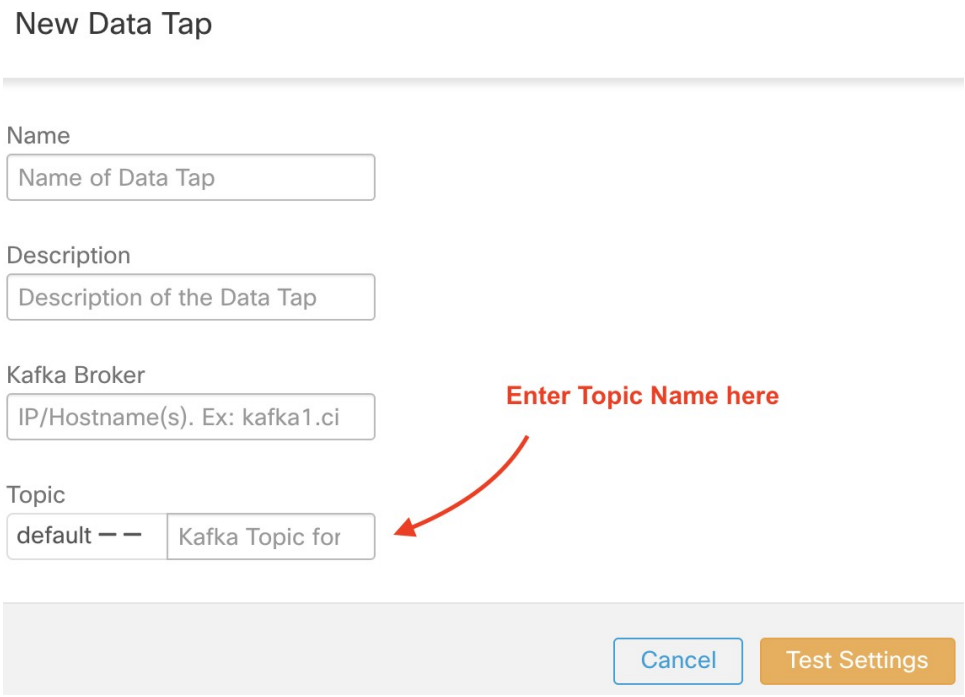


Ajout d'un nouveau surveilleur de données

Les administrateurs de dérivateurs de données peuvent cliquer sur le bouton 

pour ajouter un nouveau dérivateur de données.

Figure 496: Ajout d'un nouveau surveilleur de données

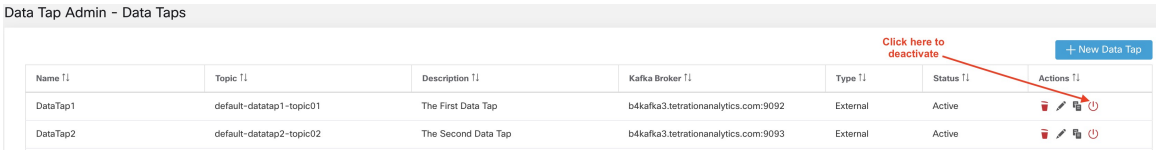


Note La modification des valeurs de surveillance de données nécessite la validation des paramètres.

Désactivation d'un surveilleur de données

Pour empêcher temporairement les messages sortants de Cisco Secure Workload, un administrateur de surveilleurs de données peut en désactiver un. Les messages destinés à ce surveilleur de données ne seront pas envoyés. Le surveilleur de données peut être réactivé à tout moment.

Figure 497: Désactivation d'un surveilleur de données



Suppression d'un surveilleur de données

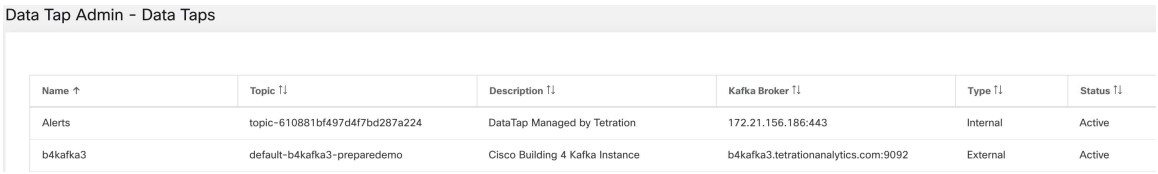
La suppression d'un surveilleur de données supprime toutes les instances des applications Cisco Secure Workload qui dépendent de cette application. Par exemple, si un utilisateur a spécifié que des alertes de conformité doivent être envoyées à surveilleur de données (DataTap) A (dans l'application alerts Cisco Secure Workload), et qu'un administrateur supprime le surveilleur de données A, l'application Alerts ne répertoriera plus le surveilleur de données A comme sortie d'alerte.

Dérivations de données gérées

Les dérivations de données gérées (MDT) sont des dérivations de données hébergées dans la grappe Cisco Secure Workload. Il est sécurisé en termes d'authentification, de chiffrement et d'autorisation. Pour envoyer et recevoir des messages des MDT, les clients doivent être authentifiés, les données envoyées de manière filaire sont chiffrées, et seuls les utilisateurs autorisés peuvent lire ou écrire des messages depuis ou à destination de Cisco Secure Workload MDT. Cisco Secure Workload fournit des certificats clients à télécharger à partir de l'interface graphique. Cisco Secure Workload utilise Apache Kafka 1.1.0 comme agent de messages, et nous recommandons que les clients utilisent des clients sécurisés compatibles avec la même version.

Les MDT sont automatiquement créés après la création de la portée racine. Un MDT Alertes est créé pour chaque portée racine. Pour récupérer des alertes de la grappe Cisco Secure Workload, vous devez utiliser l'outil MDT Alerts. Seuls les utilisateurs administrateurs de surveilleurs de données peuvent télécharger les certificats. Vous pouvez afficher les programmes MDT de votre **portée racine**.

Figure 498: Liste des dérivations de données configurées



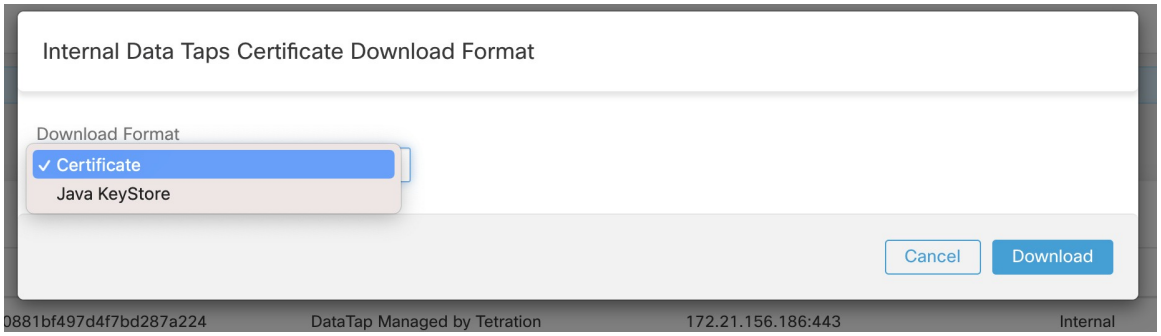
Toutes les alertes Cisco Secure Workload sont envoyées à MDT par défaut, mais peuvent être remplacées par d'autres dérivations de données.

Vous avez le choix entre deux options pour télécharger les certificats :

- Java KeyStore : le format JKS fonctionne bien avec le client Java.
- Certificat : les certificats standard sont plus faciles à utiliser avec les clients Go.

Figure 499: Télécharger des certificats

Figure 500: Types de certificats



Magasin de clés Java

Après avoir téléchargé *alerts.jks.tar.gz*, vous devriez voir les fichiers suivants qui contiennent des informations pour se connecter au MDT Cisco Secure Workload pour recevoir des messages :

- kafkaBrokerIps.txt : ce fichier contient la chaîne d'adresse IP que le client Kafka utilise pour se connecter au MDT Cisco Secure Workload.
- topic.txt : ce fichier contient la rubrique à partir de laquelle ce client peut lire les messages. Les sujets sont au format topic<root_scope_id>. Utilisez ce root_scope_id lors de la configuration d'autres propriétés du client Java.
- keystore.jks : magasin de clés que le client Kafka doit utiliser dans les paramètres de connexion indiqués ci-dessous.
- truststore.jks : le fichier de confiance que le client Kafka doit utiliser dans les paramètres de connexion indiqués ci-dessous.
- passphrase.txt : ce fichier contient le mot de passe à utiliser pour les numéros 3 et 4.

Les paramètres Kafka suivants doivent être utilisés lors de la configuration du fichier Consumer.properties (client Java) qui utilise le fichier de clés et le fichier de certificats :

```
security.protocol=SSL
ssl.truststore.location=<location_of_truststore_downloaded>
ssl.truststore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.keystore.location=<location_of_truststore_downloaded>
ssl.keystore.password=<passphrase_mentioned_in_passphrase.txt>
ssl.key.password=<passphrase_mentioned_in_passphrase.txt>
```

Lors de la configuration du consommateur Kafka dans le code Java, utilisez les propriétés suivantes :

```
Properties props = new Properties();
props.put("bootstrap.servers", brokerList);
```

```
    props.put("group.id", ConsumerGroup-<root_scope_id>);  // root_scope_id is same as
mentioned above
    props.put("key.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("value.deserializer",
"org.apache.kafka.common.serialization.StringDeserializer");
    props.put("enable.auto.commit", "true");
    props.put("auto.commit.interval.ms", "1000");
    props.put("session.timeout.ms", "30000");
    props.put("security.protocol", "SSL");
    props.put("ssl.truststore.location", "<filepath_to_truststore.jks>");
    props.put("ssl.truststore.password", passphrase);
    props.put("ssl.keystore.location", <filepath_to_keystore.jks>);
    props.put("ssl.keystore.password", passphrase);
    props.put("ssl.key.password", passphrase);
    props.put("zookeeper.session.timeout.ms", "500");
    props.put("zookeeper.sync.time.ms", "250");
    props.put("auto.offset.reset", "earliest");
```

Certificat

Si vous souhaitez utiliser des certificats, utilisez les clients Go en utilisant la bibliothèque Sarama Kafka pour vous connecter au MDT Cisco Secure Workload. Après avoir téléchargé *alerts.cert.tar.gz*, vous devriez voir les fichiers suivants :

- kafkaBrokerIps.txt : ce fichier contient la chaîne d'adresse IP que le client Kafka utilise pour se connecter au MDT Cisco Secure Workload
- topic : ce fichier contient la rubrique à partir de laquelle ce client peut lire les messages. Les sujets sont au format topic<root_scope_id>. Utilisez cet identifiant root_scope_id lors de la configuration d'autres propriétés du client Java.
- KafkaConsumerCA.cert : ce fichier contient le certificat client Kafka.
- KafkaConsumerPrivateKey.key : ce fichier contient la clé privée du consommateur Kafka.
- KafkaCA.cert : ce fichier doit être utilisé dans la liste des certificats d'autorité de certification racine dans le client Go.

Pour voir un exemple d'un client Go se connectant au MDT Cisco Secure Workload, consultez Exemple de client Go recevant les alertes de MDT.

CHAPITRE 12

Surveiller les configurations dans Cisco Secure Workload

Les options de **surveillance** qui s'offrent à vous varient en fonction de votre rôle.

Surveillance des agents

La page affiche le nombre de tous les agents surveillés dans une grappe en fonction de la portée racine actuellement sélectionnée.

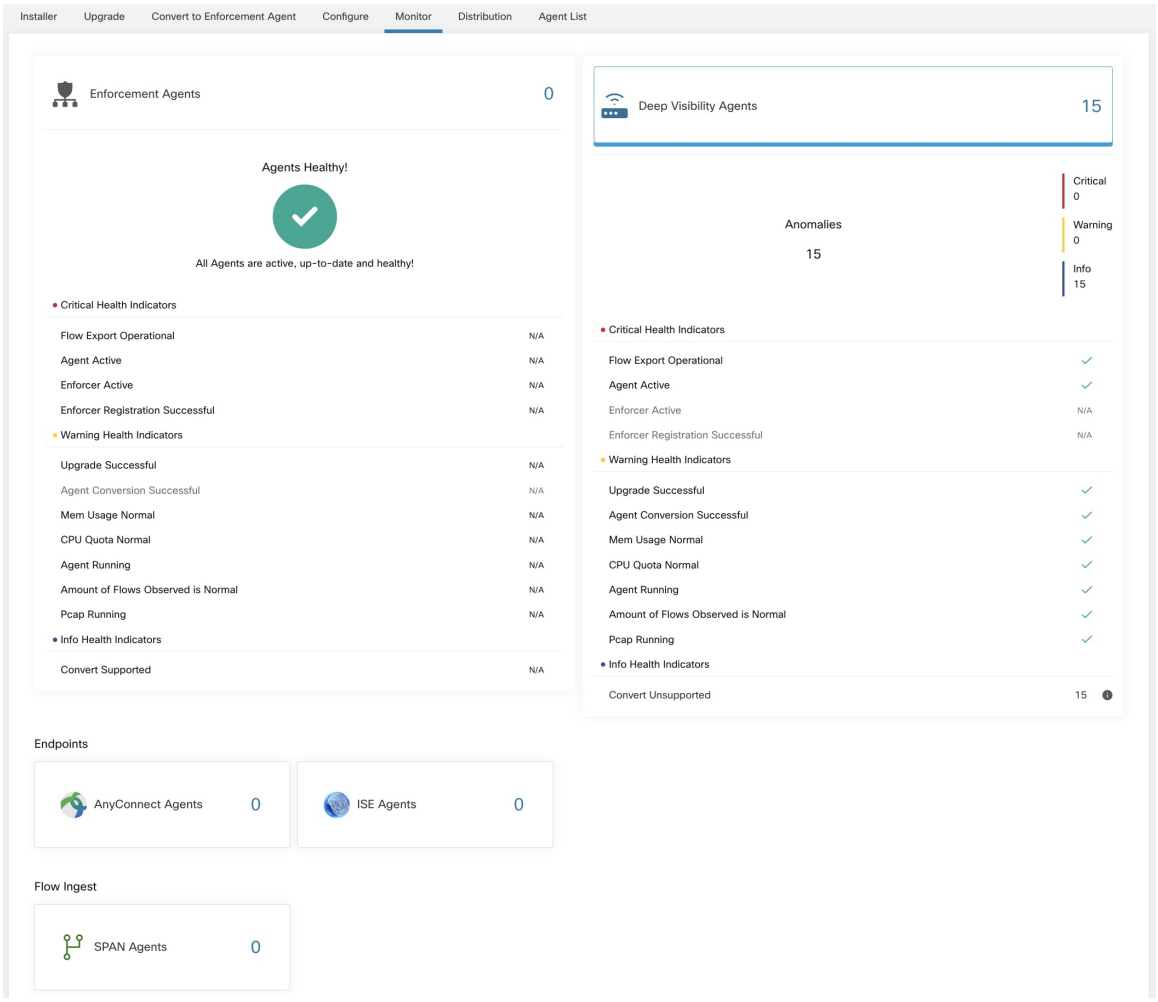
Note Le décompte total des inventaires correspond à la somme de tous les inventaires observés sur le réseau après l'application des règles de collecte.

Type de surveillance des agents

Pour surveiller les agents, cliquez sur **Manage (Gestion)** > **Agents (Agents)** dans la barre de navigation de gauche, puis cliquez sur l'onglet **Monitor** (Surveiller).

Cette page est uniquement disponible pour les utilisateurs qui ont les rôles d' **administrateur du site** et de **service d'assistance à la clientèle**. Les **propriétaires de portée** peuvent voir l'inventaire, les agents de visibilité approfondie et les agents d'exécution.

Figure 501: Nombre total d'agents installés



Le tableau suivant présente les différences entre chaque type d'agent.

Type d'agent	Description
Visibilité accrue	Fournit la précision la plus élevée en termes de séries temporelles de données de flux, de processus s'exécutant sur un hôte. La plupart des plateformes Linux et Windows sont prises en charge. See sw_agents_deployment-label
Exécution	Fournit toutes les fonctionnalités disponibles pour les agents de visibilité approfondie. En outre, les agents de mise en application peuvent définir des règles de pare-feu sur l'hôte installé.

AnyConnect	Fournit des données de flux de séries chronologiques sur les points terminaux exécutant l'agent de mobilité sécurisée AnyConnect avec module de visibilité réseau (NVM) sans nécessiter l'installation d'un agent Cisco Cisco Secure Workload. Les enregistrements IPFIX générés par NVM sont envoyés au connecteur serveur mandataire Cisco Secure Workload AnyConnect. Windows, Mac et certaines plateformes de téléphone intelligent sont prises en charge.
ISE	Fournit les métadonnées des points terminaux enregistrés auprès de Cisco ISE. Grâce à ISE pxGrid, le connecteur ISE collecte les métadonnées, enregistre les points terminaux ISE sur Cisco Secure Workload pendant que les agents ISE envoient des étiquettes en fonction des attributs extraits de l'appareil ISE et des attributs LDAP pour les utilisateurs connectés aux points terminaux.
Le tableau suivant présente un bref résumé des divers agents d'appareils fournis par Cisco Cisco Secure Workload.	
Agents d'appareil	Description
SPAN	Fournit l'analyse du flux sans nécessiter d'installation d'agent par hôte. Il s'exécute sur l'appareil de machine virtuelle Cisco Secure Workload ERSPAN. Il consomme des paquets ERSPAN provenant de n'importe quel commutateur Cisco.

Note Les agents d'appareil tels que NetFlow, NetScaler, F5, AWS et AnyConnect Proxy sont désormais pris en charge en tant que connecteurs. Pour plus d'informations sur les connecteurs, consultez Que sont les connecteurs.

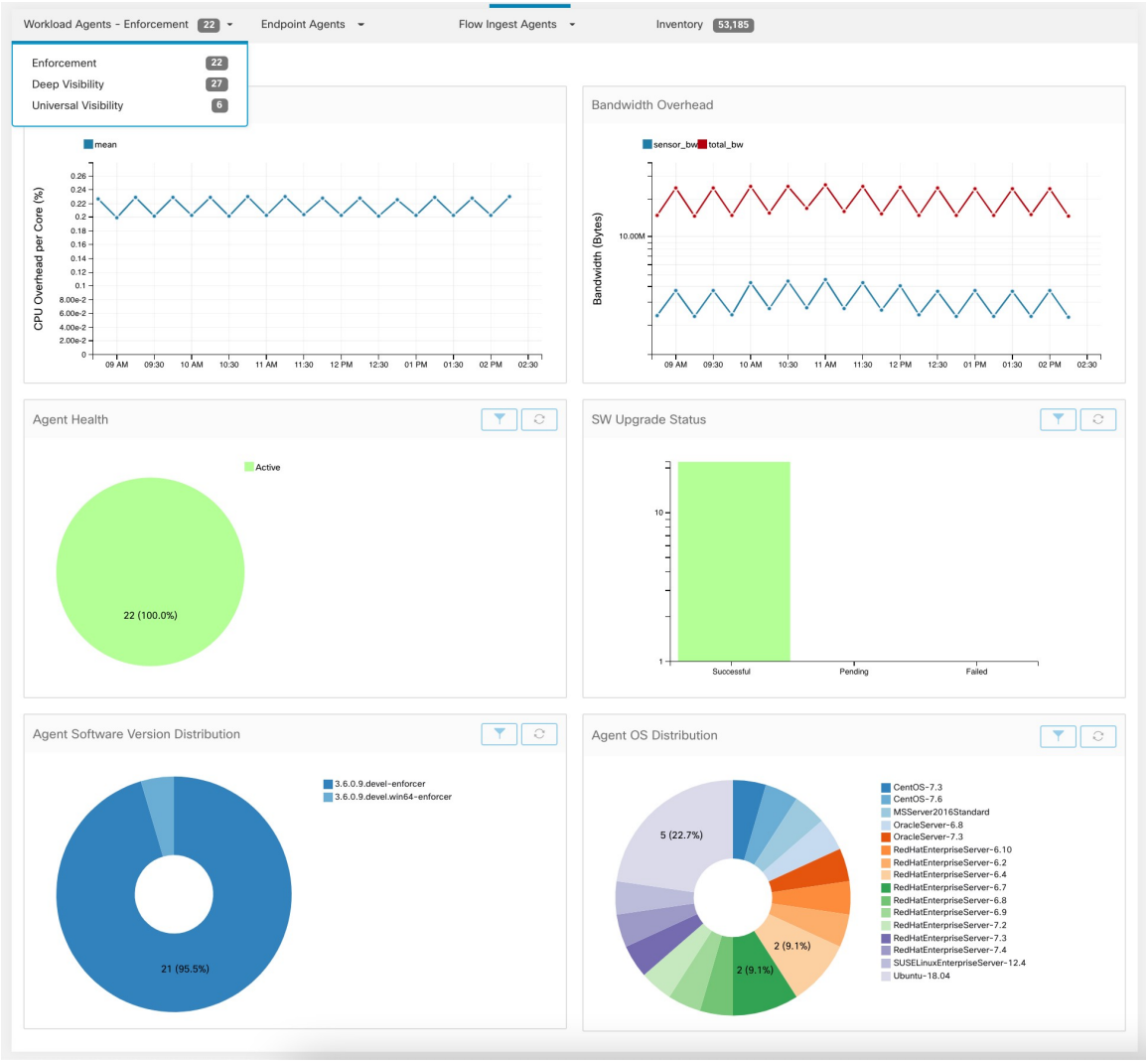
Tout bouton de type d'agent différent de zéro permet d'approfondir la répartition de chaque type d'agent.

État et statistiques de l'agent

Pour afficher les tableaux décrits dans cette rubrique, choisissez **Manage (Gestion) > Agents (Agents)**, puis cliquez sur l'onglet **Distribution (Répartition)**.

Les tableaux suivants sont disponibles pour les types d'agents de visibilité approfondie et d'application.

Figure 502: Répartition des Agents



Pour chaque type d'agent, cette page fournit un aperçu et l'intégrité des agents enregistrés, y compris la surcharge globale du processeur, la surcharge de la bande passante, les paquets manqués, la distribution du système d'exploitation/dans la version et l'état de la mise à niveau de l'agent.

Tableau de surcharge du processeur

Le tableau CPU Overhead (Surcharge du processeur) fournit une vue agrégée de la surcharge de CPU par cœur pour tous les agents. La surcharge de CPU par agent est fournie dans le cadre du Profil de la charge de travail. Ce tableau n'est disponible que pour les types d'agents de visibilité approfondie et d'application.

Tableau de surcharge de la bande passante

Le tableau Bandwidth Overhead (Surcharge de la bande passante) fournit des statistiques agrégées sur la bande passante totale et la bande passante utilisée par les agents. La surcharge de bande passante par agent est fournie dans le Profil de la charge de travail. Ce tableau n'est disponible que pour les types d'agents de visibilité approfondie et d'application.

Tableau de l'intégrité des agents

Le tableau Agent Health (Intégrité de l'agent) fournit le nombre d'agents actifs ou inactifs. Les agents actifs sont ceux qui communiquent avec le serveur de configuration pour les mises à niveau à des intervalles réguliers. L'intervalle de vérification est de 30 minutes. Si nous pouvons constater qu'un agent a manqué plus de deux périodes de vérification d'agent, il sera déclaré inactif.

Tableau des mises à jour des agents logiciels vers les dernières révisions

Chaque fois qu'un agent se connecte au serveur de configuration, l'agent fournit également sa version actuelle de RPM. Si un agent est configuré avec une version précise et n'est pas en mesure d'effectuer la mise à jour après deux périodes de vérification, l'agent sera déclaré impossible à mettre à niveau à la dernière version.

Tableau des paquets manqués par l'agent

Dans de rares cas, lorsque le volume de trafic traversant un hôte est supérieur au taux d'inspection de l'agent, certains paquets ne sont pas analysés. Le nombre de paquets manqués et le nom de l'agent correspondant sont affichés dans ce tableau.

Tableaux de répartition des versions du logiciel et du système d'exploitation de l'agent

Ces tableaux montrent la répartition des versions de l'agent et de la plateforme de système d'exploitation parente de tous les agents enregistrés auprès de la grappe Cisco Secure Workload.

État d'application

Pour afficher l'état d'application, cliquez sur **Defend (Défendre)** > **Enforcement Status (État d'application)** dans la barre de navigation à gauche de la fenêtre.

Cette page est accessible pour les administrateurs de site, les utilisateurs du service d'assistance à la clientèle et les propriétaires de portée qui souhaitent obtenir un aperçu de l'état actuel de tous les agents d'application, y compris les connecteurs infonuagiques qui appliquent une politique.

Si l'un des tableaux est rouge ou orangé, consultez la rubrique applicable :

Table 47: Tableaux de l'état d'application

Tableau	Résultat	Passer à l'action
Application par les agents activée	**Désactivée**	Vérifiez que l'application est activée dans la configuration de l'agent. Consultez Creating an Agent Config Profile, on page 83.
Configuration de politique de l'agent	**politiques périmées**	Cette situation est généralement temporaire et ne nécessite généralement aucune action. Cela se produit car un déploiement Cisco Secure Workload basé sur des étiquettes met à jour l'inventaire et les politiques de manière dynamique. Toutefois, si la situation persiste pour certaines charges de travail individuelles, communiquez avec Cisco TAC.
Politiques concrètes des agents	**Sauté**	Cela indique que les politiques n'ont pas été envoyées à certains agents.

Tip

- Pour afficher l'état de portées individuelles ou pour l'ensemble du détenteur, utilisez l'option **Filter by Scope** (filtrer par portée) dans le côté supérieur gauche de la page.
- Si les tableaux indiquent un problème, identifiez les charges de travail concernées en cliquant dans la partie correspondante du tableau.

  Le tableau affiche les charges de travail concernées.

  Pour voir les options de filtrage, vous pouvez également cliquer sur le bouton (i) dans la zone **Filter** (Filtrer) sous les tableaux.
- Pour afficher un grand nombre de détails supplémentaires, cliquez sur le lien IP address (adresse IP) dans la liste filtrée des charges de travail pour afficher la page Workload Profile (Profil de charge de travail).

Le tableau suivant décrit les champs affichés dans le tableau de l'état d'application.

Champ	Description
Nom de l'hôte	Nom d'hôte de la charge de travail.
Adresse	Les adresses IP de toutes les interfaces de la charge de travail
Enforcement Enabled	Indique si l'application est activée ou non sur l'agent.
Concrete Policies in Sync	Ceci indique si la version souhaitée de politiques concrètes est actuellement appliquée sur l'agent.
Politiques concrètes	Si cette valeur indique **Skipped** (ignoré) pour un hôte, cela signifie que la limite des politiques est atteinte pour l'agent sur cet hôte. (Consultez Limites liées aux politiques, on page 1172.)
Policy Count	Le nombre de politiques concrètes sur l'agent.
État	L'état de la dernière application de configuration de politiques. Si l'état est **CONFIG_SUCCESS**, cela indique que la version actuelle est appliquée sans problème.

État d'application pour les connecteurs infonuagiques

Si vous avez configuré les connecteurs infonuagiques AWS ou Azure :

L'état d'application de toutes les interfaces est affiché dans la page d'état d'application. Si les politiques sont appliquées avec succès, elles sont synchronisées, sinon les messages d'erreur correspondants s'affichent.

Le nombre de politiques dans la page d'état d'application est issu de la comptabilité Cisco Secure Workload, mais pas de la gestion de règles AWS ou Azure.

(AWS uniquement) Le champ de nom d'hôte sur cette page est dérivé du DNS public. Si le DNS public n'est pas activé sur le VPC donné, le champ de nom d'hôte est vide.

Suspendre les mises à jour des politiques

Caution Cette option met en pause les mises à jour de politiques pour TOUTES les charges de travail dans TOUTES les portées.

Cette fonctionnalité nécessite des privilèges d'administrateur de site ou de service d'assistance à la clientèle.

Pour suspendre les mises à jour des règles pour tous les points terminaux d'application dans toutes les portées :

1. Dans le volet de navigation, choisissez **Defend (Défendre)** > **Enforcement (Mise en application)** .
2. Cliquez sur l'état à côté de **Policy Updates** (Mises à jour des politiques) .
3. Lisez et acceptez la mise en garde.

Figure 503: Les règles de pare-feu sont mises à jour en permanence

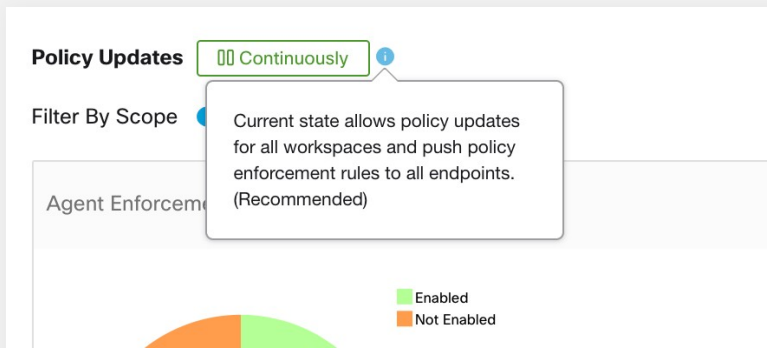


Figure 504: Les mises à jour des règles de pare-feu sont suspendues

CHAPITRE 13

Analyse des rapports d'informations sur les menaces

Le tableau de bord **Threat Intelligence** (Informations sur les menaces) fournit l'ensemble des données les plus récentes au processus de Cisco Secure Workload qui identifie et met en quarantaine les menaces en inspectant les charges de travail du centre de données par rapport aux adresses de commande et de contrôle des logiciels malveillants connues de l'extérieur, aux failles de sécurité dans les processus et à l'emplacement géographique.

Pour gérer les renseignements sur les menaces, dans le volet de navigation, choisissez **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Threat Intelligence (Informations sur les menaces)**.

Le tableau de bord des informations sur les menaces affiche l'état mis à jour des ensembles de données d'informations sur les menaces. Ces ensembles de données sont mis à jour automatiquement.

Avertissement La fonctionnalité de renseignements sur les menaces nécessite une connexion aux serveurs Cisco Cisco Secure Workload pour se mettre à jour automatiquement. Votre requête HTTP sortante Enterprise peut nécessiter :

- D'autoriser le domaine suivant dans les règles de sortie du pare-feu d'entreprise : `uas.tetrationcloud.com`
- De configurer votre connexion HTTP sortante.

Dans les environnements sans connexion sortante, importez directement les ensembles de données. Pour en savoir plus, consultez la section **Chargements manuels**.

Tableau 48 : Ensembles de données

Jeu de données	Description
CVE de NVD	Défaillances logicielles liées à la sécurité, note de base CVSS, configuration de produits vulnérables et catégorisation des vulnérabilités
Zone géographique MaxMind	L'identification de l'emplacement et d'autres caractéristiques des adresses IP source
RDS NIST	Ensemble de données de référence NIST de signatures numériques d'applications logicielles connues et traçables

Jeu de données	Description
Équipe Cymru	Informations sur plus de 3 000 adresses IP de commandes et de contrôles pour réseaux de zombies
Verdict de condensé	Verdict de Cisco Secure Workload sur les condensés de processus (uniquement disponible avec la sectionMises à jour automatiques).

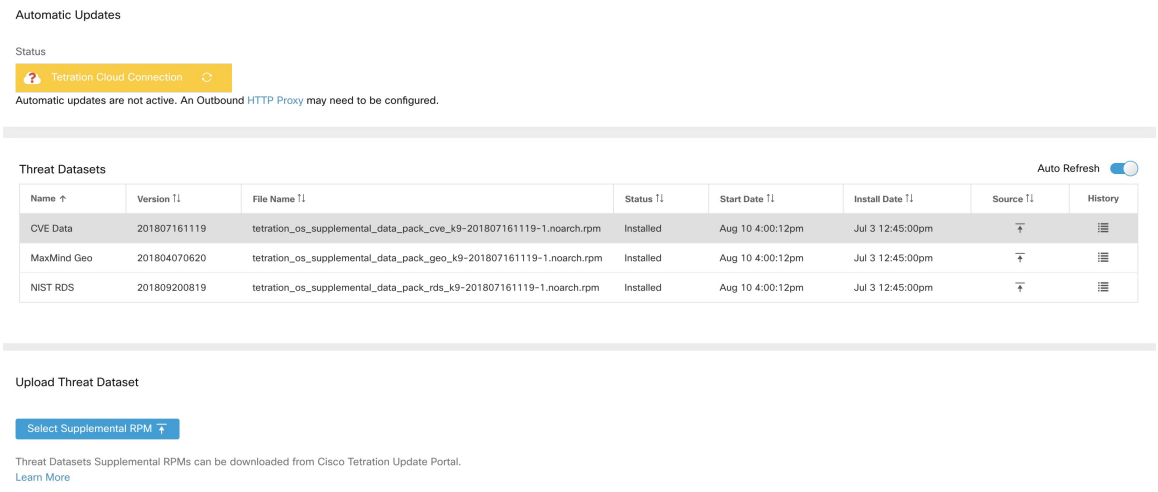
Remarque Si l'ensemble de données MaxMind Geo est téléversé manuellement dans une version antérieure, vous devez téléverser à nouveau le RPM correspondant pour afficher l'emplacement et les informations connexes sur la page Flow Visibility (Visibilité des flux).

- Mises à jour automatiques, on page 826
- Chargements manuels, on page 827

Mises à jour automatiques

Les mises à jour des ensembles de données sur les menaces sont déclenchées par l'appareil pour se synchroniser avec l'ensemble de données mondial hébergé sur Internet à l'adresse uas.tetrationcloud.com, tous les jours entre 3 h et 4 h UTC. L'ensemble mondial de données est actualisé chaque semaine, le vendredi ou le lundi. Le tableau de bord des informations sur les menaces répertorie les ensembles de données et la date à laquelle l'ensemble de données a été mis à jour pour la dernière fois.

Figure 505: Tableau de bord



Chargements manuels

Attention **Planification des téléchargements manuels** : les fichiers RPM des ensembles de données sont publiés sur une mise à jour hebdomadaire du portail Cisco Secure Workload. Il est recommandé d'installer les dernières versions régulièrement en configurant un calendrier l'administrateur.

Téléchargement des ensembles de données mis à jour

Les ensembles de données peuvent être téléchargés à partir du portail des mises à jour Cisco Secure Workload.

Chargement manuel d'ensembles de données

Pour charger les fichiers RPM d'ensembles de données :

Before you begin

Connectez-vous en tant **qu'administrateur de site** ou **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Manage(Gestion)** > **Service Settings(Paramètres de service)** > **Threat Intelligence** (Informations sur les menaces).

Étape 2 Dans la section **Upload Threat Dataset** (Charger l'ensemble de données sur les menaces), cliquez sur **Select Supplemental RPM** (Sélectionner un RPM supplémentaire).

Étape 3 Chargez le fichier RPM téléchargé à partir du portail de mise à jour Cisco Secure Workload.

Étape 4 Cliquez sur **Upload** (Téléverser).

Le processus de téléversement du RPM est lancé et l'état est affiché dans une barre de progression. Après le téléchargement, le fichier RPM est traité et installé en arrière-plan. La table est mise à jour une fois l'installation terminée.

Figure 506: Ensembles de données sur les menaces

CHAPITRE 14

Tableau de bord de production de rapports

Le tableau de bord de création de rapports, conçu pour les responsables, les administrateurs réseau et les analystes de sécurité, fournit des représentations visuelles de l'état des flux de travail critiques, des fonctionnalités de dépannage et des fonctionnalités de création de rapports. Dans le volet de navigation, choisissez **Reporting (Création de rapport)** > **Reporting Dashboard (Tableau de bord de création de rapport)** pour accéder au tableau de bord.

• Tableau de bord de production de rapports, on page 829

Tableau de bord de production de rapports

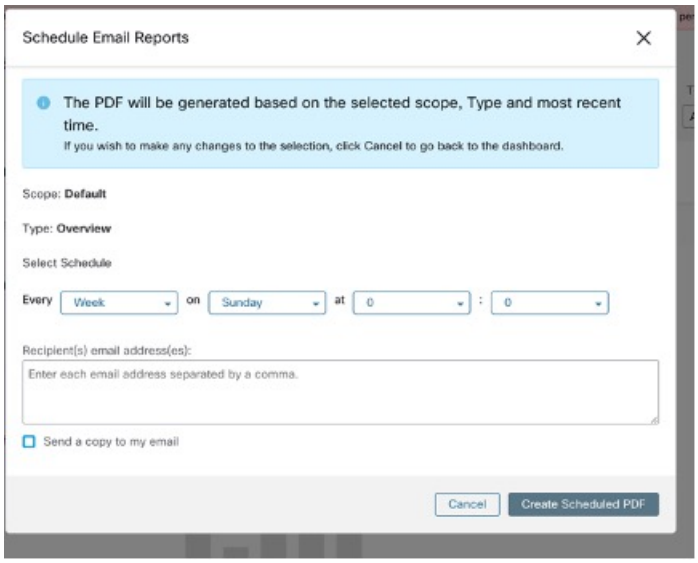
Les sections ci-dessous fournissent un aperçu des rapports et la façon de planifier et d'envoyer des rapports par courriel.

Planifier des rapports par courriel

Pour générer un rapport, choisissez l'une des options suivantes :

- **Télécharger** : après avoir généré un rapport, vous pouvez télécharger et enregistrer une copie du rapport pour consultation future.
- **Courriel** : si vous choisissez l'option des rapports par courriel, un courriel sera envoyé aux destinataires avec le rapport en pièce jointe.
- **Planifier** : vous avez le choix entre deux options pour planifier la production d'un rapport.
  - Tous les jours
  - Hebdomadaire

    Pour planifier la production d'un rapport, saisissez les détails de la planification pour déclencher le rapport. Sélectionnez Chaque semaine ou Tous les jours, saisissez le jour et l'heure, ainsi que les adresses courriel des destinataires. Cliquez sur **Create Scheduled PDF** (Créer un PDF planifié) pour enregistrer les détails.



Note Si la planification du rapport échoue, vérifiez le calendrier pour déterminer les adresses de courriel incorrectes ou les date et heure saisies de façon incorrecte.

Pour accéder aux planifications de rapports générées précédemment, choisissez **Generated Reports > Schedules** (Rapports générés > Planifications). Si la planification du rapport échoue, vérifiez le calendrier pour déterminer toute adresse de courriel incorrecte ou les date et heure incorrectes.

Note Le nombre maximal de planifications que vous pouvez stocker dans le tableau de bord des planifications est de cinq.

Aperçu

La section Aperçu fournit des renseignements en temps réel sur les informations relatives aux flux du réseau, les politiques de sécurité, le rendement du système et les menaces à la sécurité. Elle permet aux analystes de sécurité et aux administrateurs réseau de prendre des décisions éclairées et de prendre des mesures pour protéger leurs ressources de données.

Résumé de la segmentation

Les espaces de travail sont les pierres angulaires de la découverte, de l'application et de la gestion des politiques et de leur mise en application au sein de la grappe. Vous pouvez définir les adhésions à la segmentation en sélectionnant la portée appropriée.

Le résumé de la segmentation saisit les détails de configuration de chaque espace de travail, pour toutes les activités liées aux politiques, telles que la définition, l'analyse et l'application des politiques pour une portée particulière dans l'espace de travail ou les espaces de travail associés à cette portée.

Le graphique affiche un résumé des différentes politiques associées aux espaces de travail.

Figure 507: Résumé de la segmentation

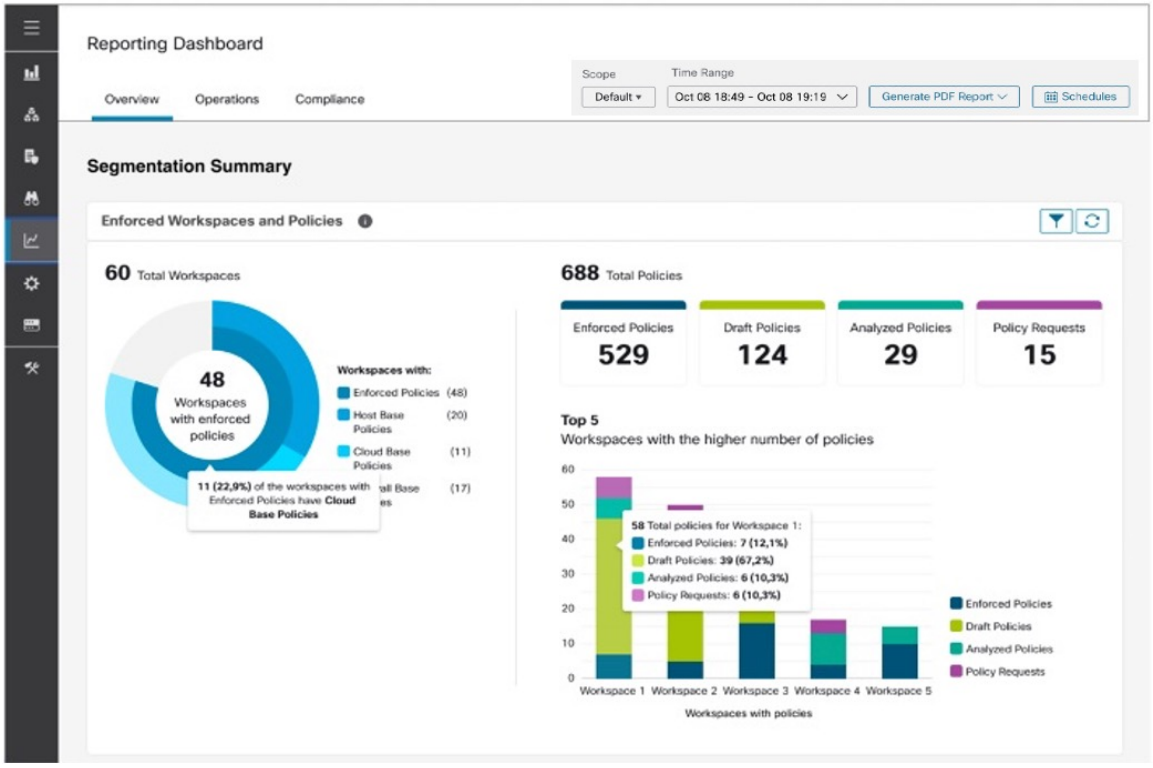
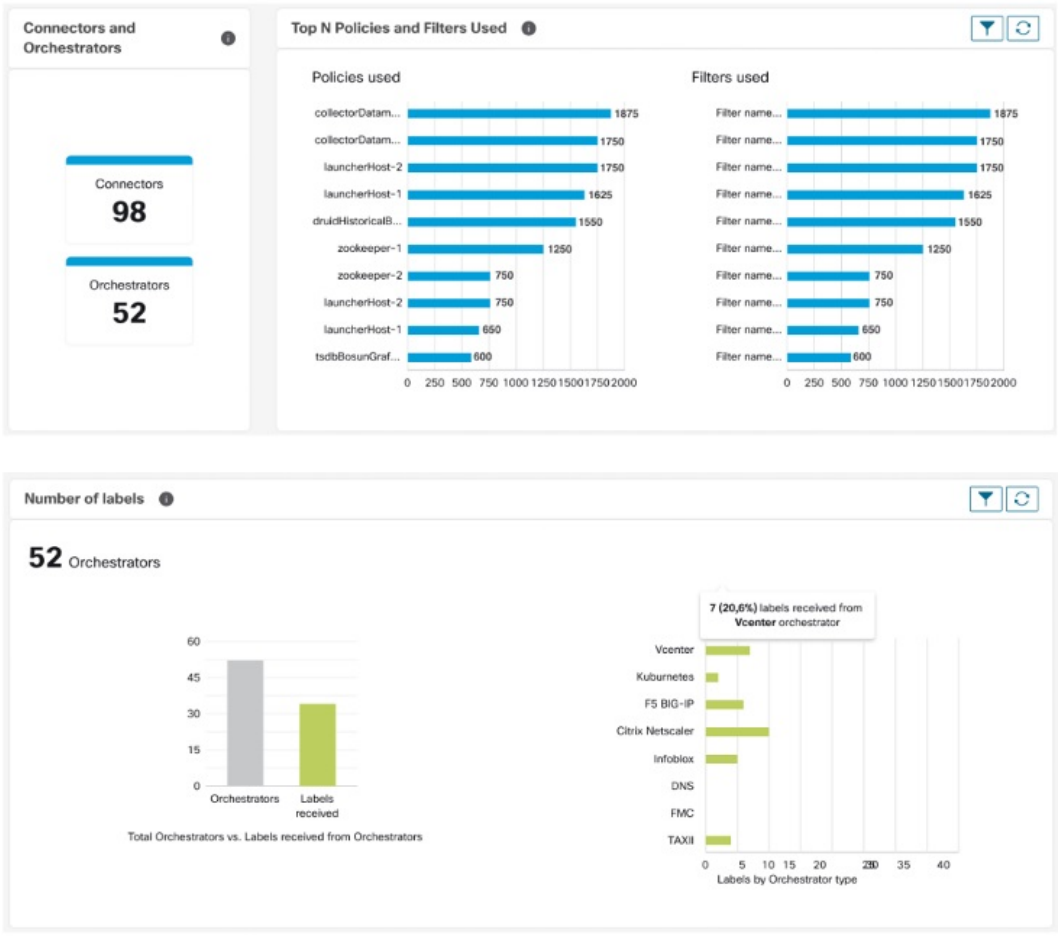


Figure 508: Connecteurs et orchestrateurs

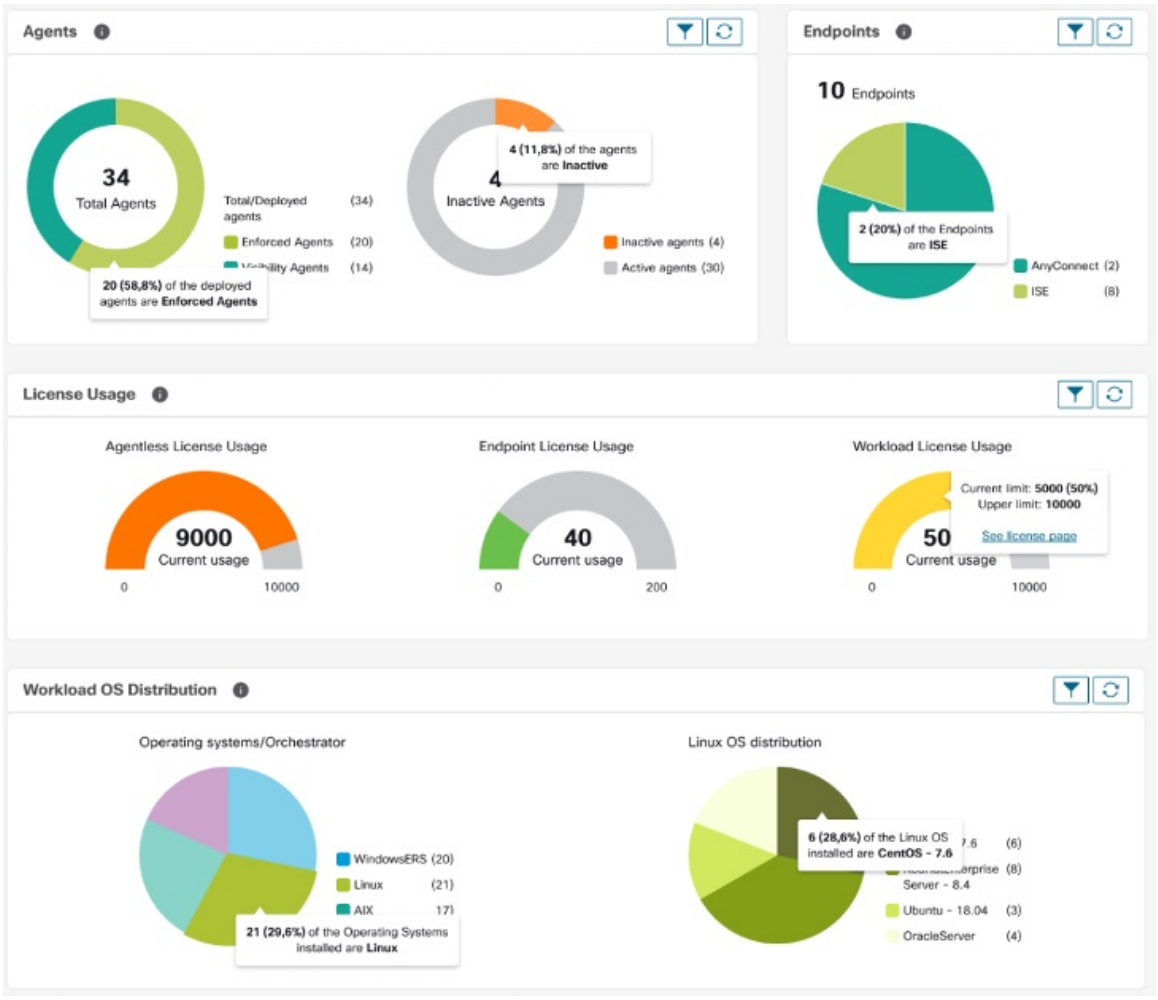


Résumé de la charge de travail

Le résumé de la charge de travail fournit les détails suivants sur les agents déployés sur un ou plusieurs serveurs et points terminaux de l'infrastructure :

- Les agents surveillent et recueillent des informations sur les flux du réseau.
- Les agents appliquent les politiques de sécurité avec les règles de pare-feu sur les hôtes installés.
- Les agents communiquent l'état de la charge de travail.
- Les agents reçoivent des mises à jour des politiques de sécurité.

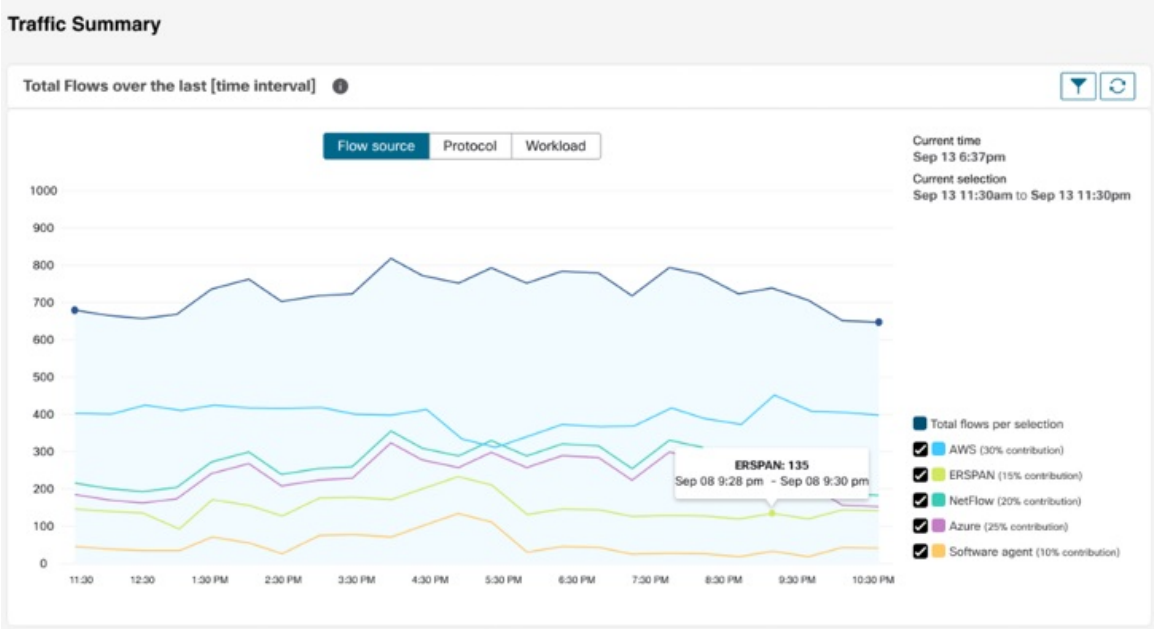
Figure 509: Résumé de la charge de travail



Résumé du trafic

Le résumé du trafic contient les observations de flux de chaque flux. Chaque observation de la source de flux suit le nombre de paquets, d'octets et d'autres mesures relatives aux flux.

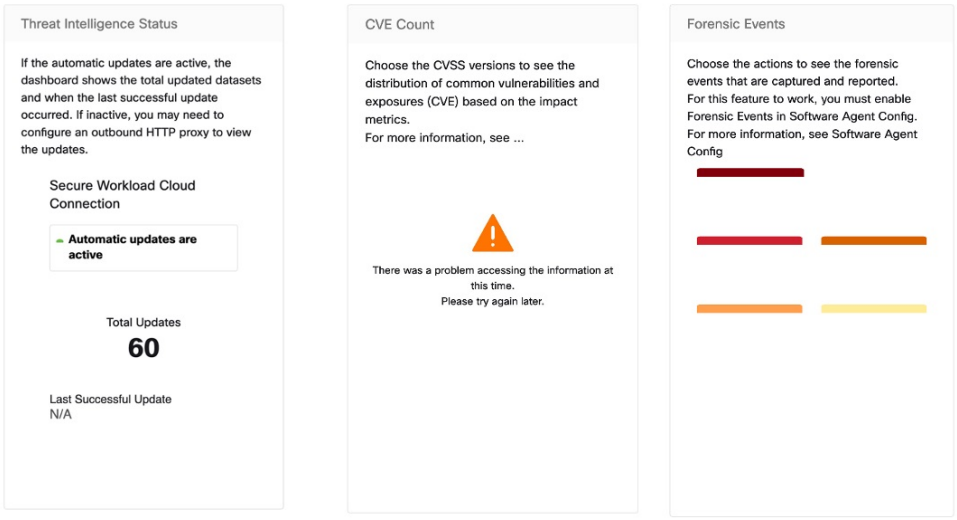
Figure 510: Résumé du trafic



Résumé de la sécurité

Le résumé de la sécurité fournit l'état des renseignements sur les menaces (la dernière fois que les mises à jour de l'état des renseignements sur les menaces ont été reçues est indiquée), le nombre de CVE et la distribution des événements criminalistiques.

Figure 511: Résumé de la sécurité

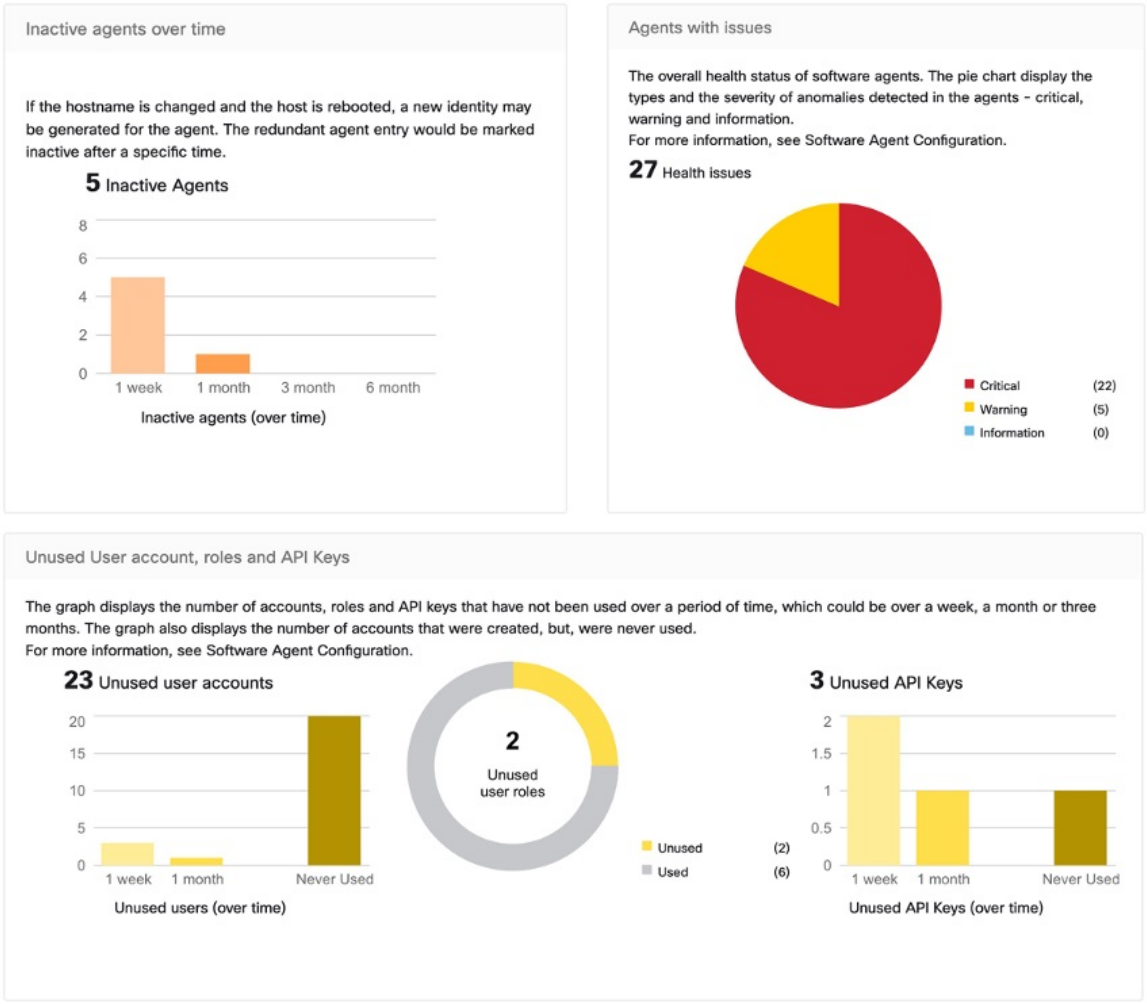


Operation (Opération)

Résumé de la charge de travail

Le résumé de la charge de travail fournit une vue du nombre total d'agents déployés sur un ou plusieurs serveurs et points terminaux du réseau. Les agents surveillent et recueillent des renseignements sur les flux de réseau, appliquent les politiques de sécurité à l'aide de règles de pare-feu sur les hôtes installés, communiquent l'état de la charge de travail et reçoivent les mises à jour des politiques de sécurité.

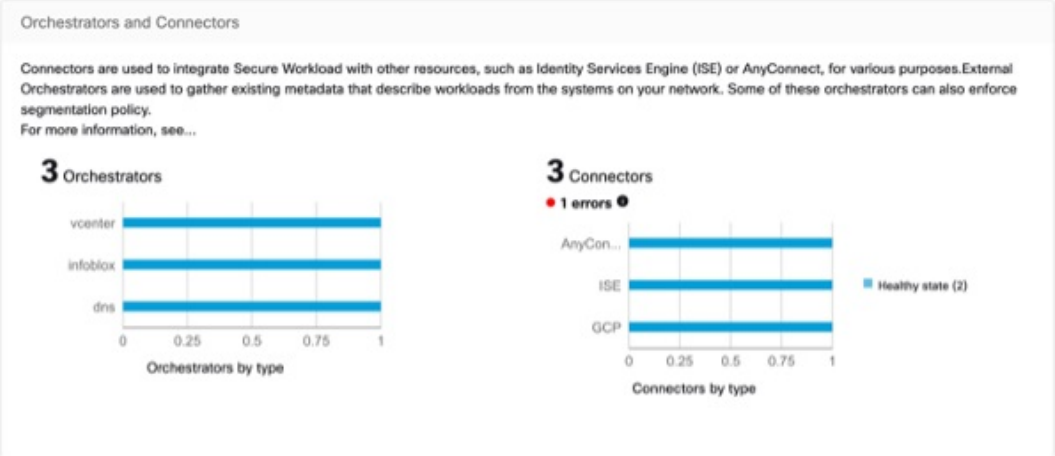
Figure 512: Résumé de la charge de travail



Résumé de la télémétrie

De nombreux connecteurs qui sont déployés sur l'appliance virtuelle recueillent la télémétrie à partir de divers points du réseau, ces connecteurs doivent être à l'écoute sur des ports spécifiques de l'appareil.appliance. Les connecteurs peuvent acquérir des journaux de flux si vous avez configuré ces derniers pour vos groupes de sécurité spécifiques. Vous pouvez également utiliser les données de télémétrie pour la génération de politiques de visualisation et de segmentation.

Figure 513: Résumé de la télémétrie



Résumé de la grappe

Les administrateurs de site peuvent accéder à la page d'état de la grappe, mais les actions ne peuvent être effectuées que par les utilisateurs du service d'assistance à la clientèle. Il indique l'état de tous les serveurs physiques dans le châssis (rack) Cisco Secure Workload.

La durée de traitement et de conservation des grappes fait référence à la durée pendant laquelle les données sont stockées et traitées dans une grappe. Les durées de traitement et de conservation spécifiques dépendent des exigences de la charge de travail et des politiques de l'organisation.

Il est important de prendre en compte les exigences de temps de traitement lors de la configuration de la grappe, car cela peut avoir une incidence sur la capacité de stockage et la puissance de traitement nécessaires pour répondre aux besoins de la charge de travail.

La durée de conservation fait référence à la durée pendant laquelle les données sont conservées dans une grappe. Pour certaines charges de travail, les données peuvent devoir être conservées à des fins réglementaires ou de conformité, tandis que pour d'autres, elles peuvent être supprimées après avoir été traitées. Il est important d'établir des politiques de rétention pour la charge de travail afin de garantir que les données sont conservées pendant la durée appropriée, puis supprimées de manière sécurisée pour empêcher tout accès non autorisé.

Figure 514: Résumé de la grappe

Résumé de la segmentation

La segmentation ou les espaces de travail d'application sont les éléments constitutifs de la découverte, de l'application et de la gestion des politiques et de leur mise en application au sein de la grappe. Le résumé de segmentation saisit les détails de configuration pour chacun des espaces de travail d'application mis en œuvre, le n° des espaces de travail avec et sans application, des politiques qui ont été activées ou désactivées, des espaces de travail qui ont des politiques à jour ou non synchronisées, avec ou sans politiques en cours d'élaboration.

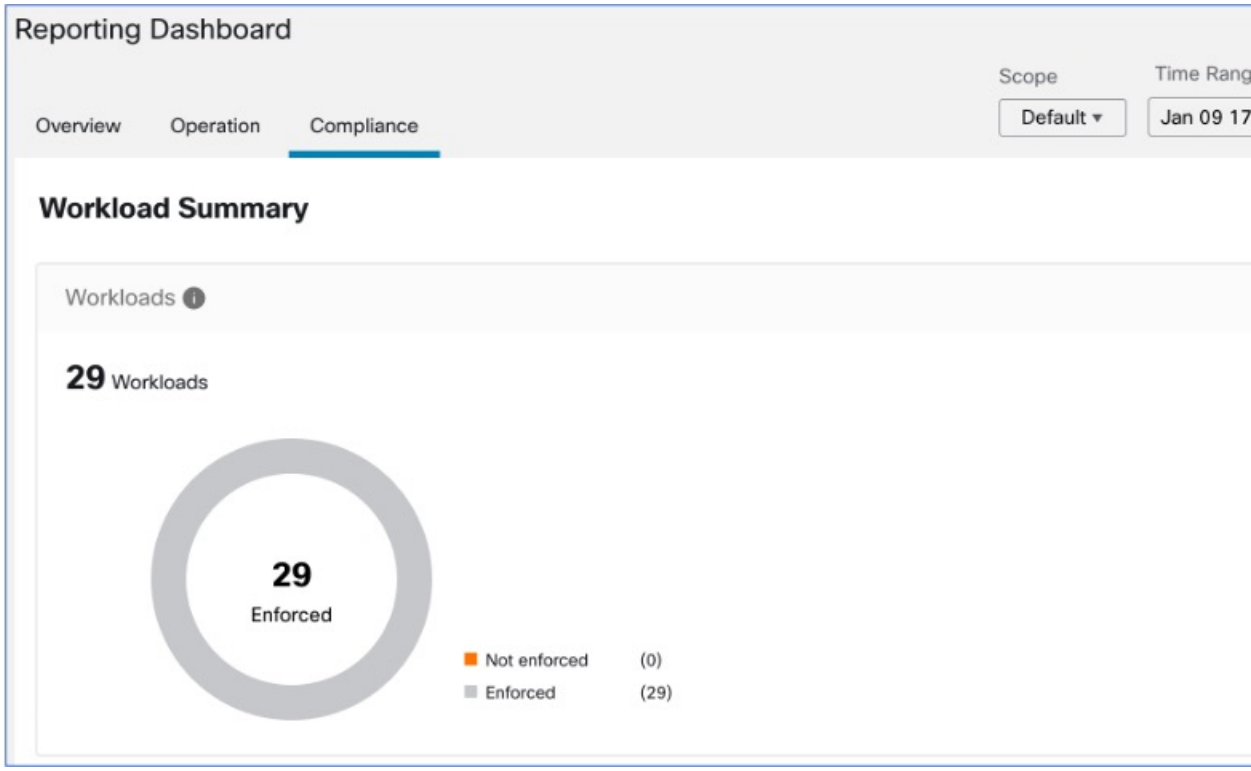
Figure 515: Résumé de la segmentation

Conformité

Résumé de la charge de travail

Le résumé de la charge de travail fournit une vue du nombre total d'agents déployés sur un ou plusieurs serveurs et points terminaux de l'infrastructure. Les agents surveillent et recueillent des renseignements sur les flux de réseau, appliquent les politiques de sécurité à l'aide de règles de pare-feu sur les hôtes installés, communiquent l'état de la charge de travail et reçoivent les mises à jour des politiques de sécurité.

Figure 516: Résumé de la charge de travail



Résumé de la sécurité

Configurez vos événements criminalistiques; une fois configurées, toutes les tactiques sont affichées sans aucune règle, avec un nombre de 0. Sélectionnez une ou plusieurs règles criminalistiques pour effectuer la sélection au niveau de la tactique. Sélectionner une tactique sélectionne toutes les règles qu'elle contient. Les règles par défaut de la fonction MITRE ATT&CK sont fournies pour envoyer des alertes techniques à partir du cadre de la fonction MITRE ATT&CK.

Figure 517: Résumé de la sécurité

Espaces de travail avec des CVE

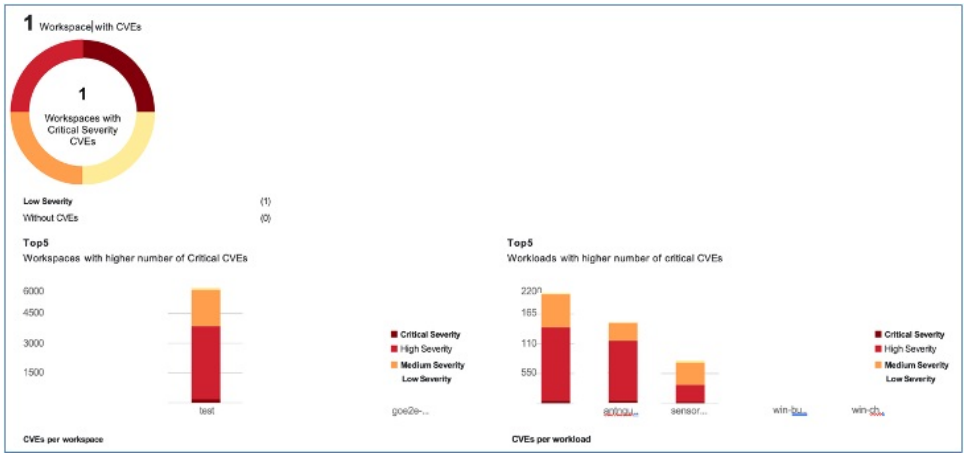
En fonction de la portée sélectionnée et du système de notation (v2 ou v3), le décompte des vulnérabilités et expositions communes (CVE) met en évidence les vulnérabilités (classées en fonction des notes) sur les

charges de travail dans les portées sélectionnées. Consultez la répartition des espaces de travail et des charges de travail avec le plus grand nombre de CVE critiques.

Les paquets logiciels d'une charge de travail pourraient être associés à des vulnérabilités connues (CVE). Le système Common Vulnerability Scoring System (CVSS) est utilisé pour évaluer l'impact d'une CVE. Une CVE peut avoir une note CVSS v2 et CVSS v3. Pour calculer la note de vulnérabilité, prenez en compte CVSS v3 s'il est disponible, sinon CVSS v2 est pris en compte.

La note de vulnérabilité pour une charge de travail est dérivée des notes des logiciels vulnérables détectés sur cette charge de travail. La note de vulnérabilité de la charge de travail est calculée sur la base des notes CVSS et des données du fournisseur. L'équipe de recherche en sécurité peut procéder à des ajustements lorsque les données sont manquantes ou inexactes. Plus la gravité de la vulnérabilité la plus grave est élevée, plus la note est faible.

Figure 518: Espaces de travail avec des CVE



CHAPITRE 15

Afficher le Tableau de bord de sécurité

Ce chapitre fournit des informations sur la note de sécurité, les catégories de note de sécurité et les détails de la note au niveau de la portée présentés dans le tableau de bord de sécurité.

Le tableau de bord de la sécurité présente des évaluations de sécurité exploitables en rassemblant plusieurs signaux disponibles dans Cisco Secure Workload, ce qui aide à comprendre la position actuelle de la sécurité et à l'améliorer. Le tableau de bord de la sécurité sert de tremplin vers de nombreuses analyses plus approfondies dans Cisco Secure Workload, telles que la recherche de flux, la recherche d'inventaire, la découverte automatique des politiques et la criminalistique.

Afficher le Tableau de bord de sécurité

Pour afficher le Tableau de bord de sécurité, dans le volet de navigation, choisissez **Overview** (Aperçu).

Note de sécurité

La note de sécurité est un nombre compris entre 0 et 100 et indiquant la position de sécurité dans une catégorie. Une note de 100 est la meilleure note et une note de 0 est la pire. Les notes proches de 100 sont les meilleures.

Le calcul de la note de sécurité prend en compte les vulnérabilités des logiciels installés, la cohérence des condensés de processus, les ports ouverts sur différentes interfaces, les événements criminalistiques et d'anomalies de réseau, et la conformité ou la non-conformité aux politiques.

Catégories de notes de sécurité

Il existe six catégories de notes différentes. La plupart des aspects de sécurité d'une charge de travail sont pris en compte pour déterminer ces catégories.

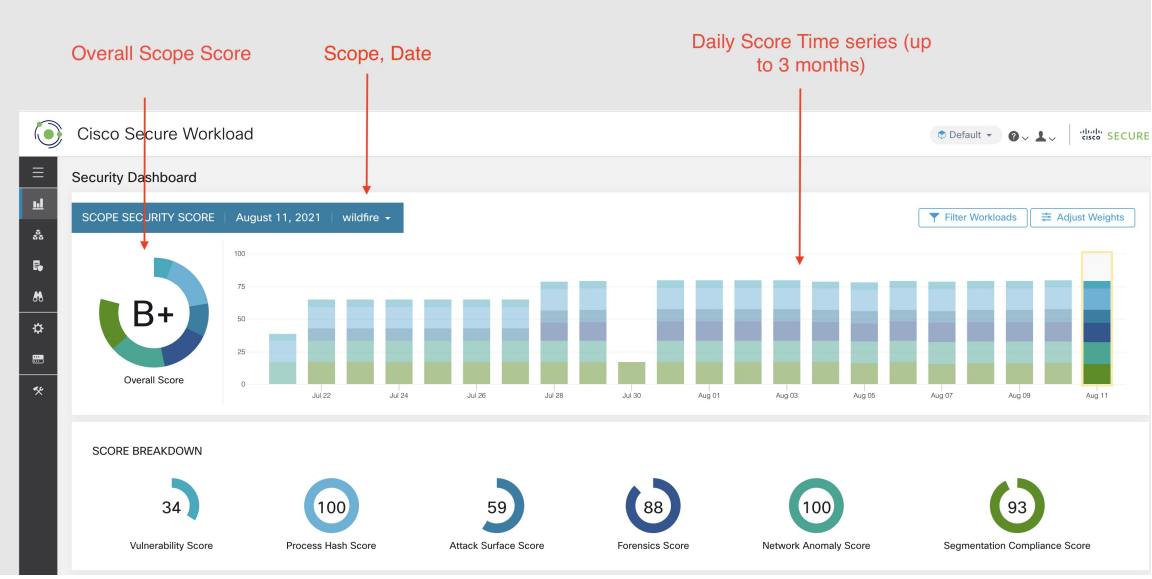
- **Note de vulnérabilité** : les vulnérabilités des paquets installés sur une charge de travail sont utilisées pour l'évaluation.
- **Note de condensé de processus** : La cohérence (et l'anomalie) des condensés de processus ainsi que des condensés de processus bénins et marqués sont utilisées pour l'évaluation.
- **Note de la surface d'attaque** : le processus peut avoir un ou plusieurs ports ouverts sur plusieurs interfaces pour rendre les services disponibles. Les ports ouverts inutilisés sont utilisés pour l'évaluation.
- **Note criminalistique** : la gravité des événements criminalistiques sur une charge de travail est utilisée pour l'évaluation.
- **Note d'anomalie de réseau** : la gravité des événements d'anomalie de réseau sur une charge de travail est utilisée pour l'évaluation.
- **Note de conformité de la segmentation** : la conformité (politiques autorisées) et les violations (politiques échappées) des politiques découvertes automatiquement sont utilisées pour l'évaluation.

Vue générale

Le tableau de bord de sécurité dispose de notes au niveau de la portée sélectionnée. Il existe une note globale avec des séries chronologiques et une ventilation des notes. Les détails des notes pour les six catégories de notes de la portée sélectionnée s'affichent.

Détails de la note au niveau de la portée

Les détails de la note au niveau de la portée s'affichent en haut du tableau de bord.



Les renseignements détaillés suivants sont affichés :

- **Note globale de la portée** : note globale de la portée sélectionnée.
- **Séries chronologiques de notes quotidiennes** : séries chronologiques empilées pouvant aller jusqu'à 3 mois.
- **Répartition des notes** : répartition des notes des catégories pour la journée sélectionnée de la série chronologique.

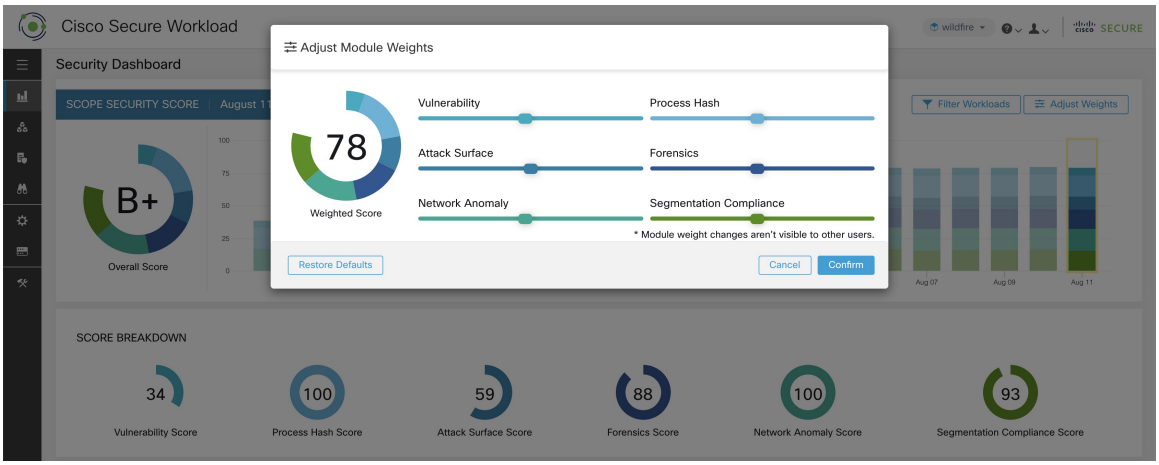
Note globale

La note globale est représenté par une lettre de **A+, A,…, F**, **A+** étant considéré comme la meilleure note et **F** comme la plus mauvaise. Elle est affichée sous forme de graphique en anneau, chaque tranche (représentée par un code de couleur) représentant une catégorie de note.

La note globale correspond à la moyenne pondérée des six catégories de note. Par défaut, toutes les pondérations sont égales. Si une note est **S.O.**, elle est considérée comme à 0 dans le calcul de la note globale.

$$\text{Overall score} = \frac{\sum W_{category} \times Score_{category}}{\sum W_{category}}$$

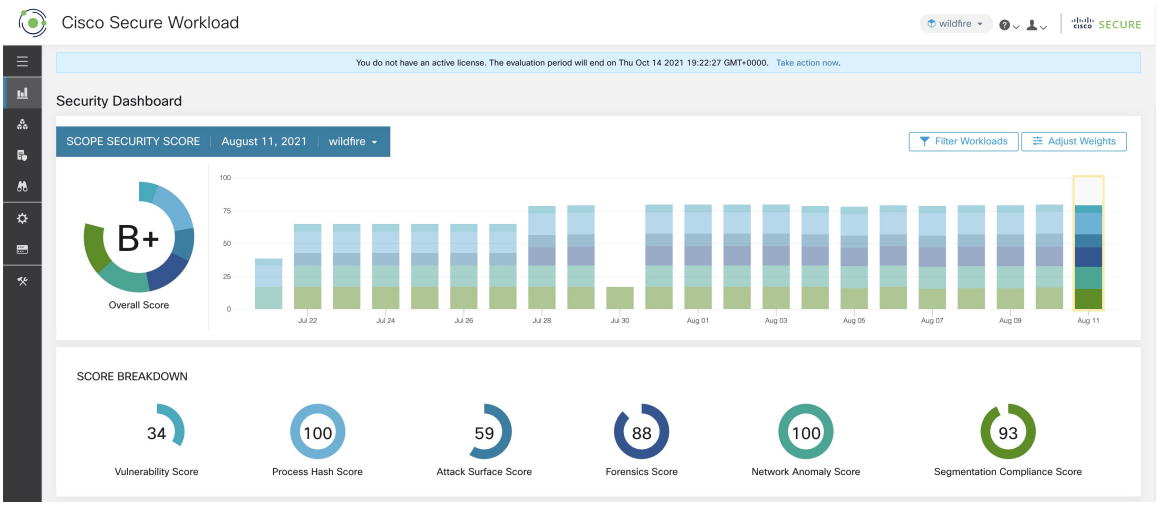
La pondération peut être ajustée à l'aide des curseurs du module **d'ajustement de la pondération**. Chaque utilisateur peut définir ses propres ajustements de pondération, ce qui aide à harmoniser les notes avec vos priorités.



Important : Si le score est **S.O.**, il est considéré comme à **0** dans le calcul de la note globale.

Séries chronologiques quotidiennes

Séries chronologiques empilées pouvant aller jusqu'à trois mois. Cela permet de suivre la situation en matière de sécurité sur une longue période. Chaque pile représente une note globale pour une journée. Chaque segment de la pile est une catégorie qui est représenté par une couleur différente. Vous pouvez cliquer sur un jour pour obtenir la ventilation de la note pour la journée.



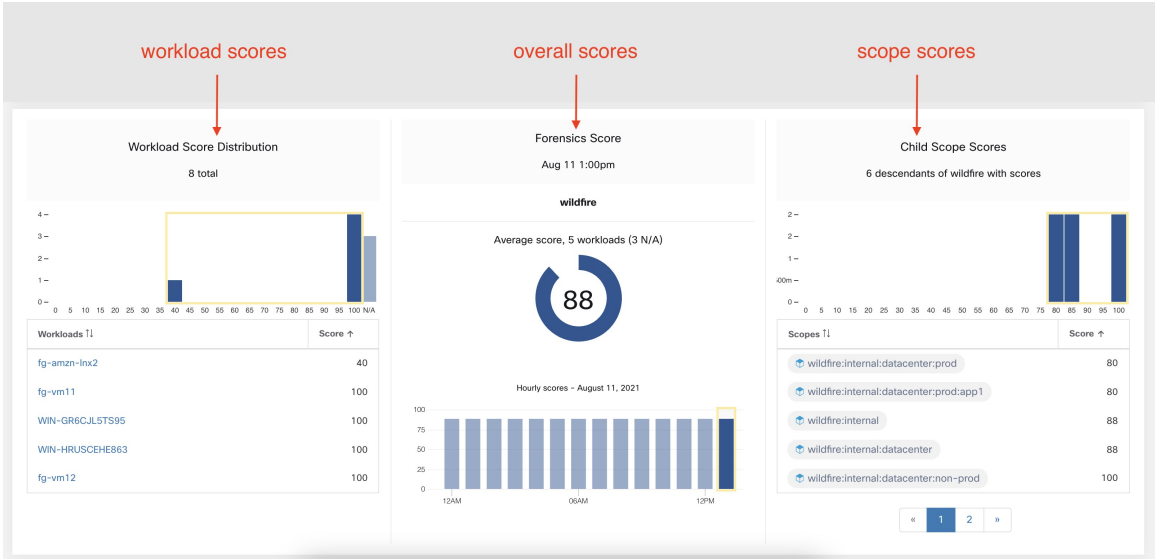
Répartition de la note

La répartition de la note affiche le résultat pour les six catégories pour la journée sélectionnée dans la série chronologique. Une note **S.O.** indique que la note n'est pas disponible. Elle comptera pour 0 dans le calcul de la note globale.

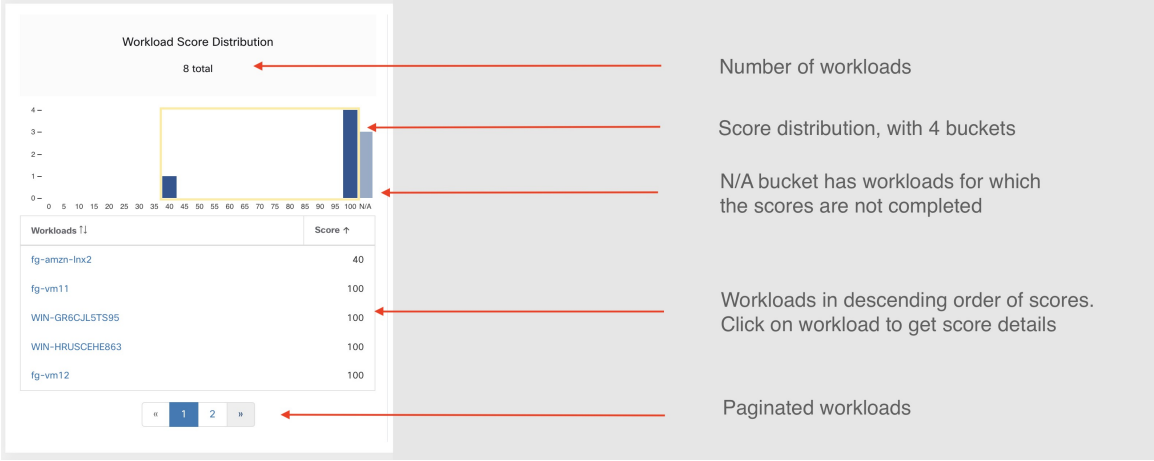
Important Si la note est **S.O.**, elle est considérée comme **0** dans le calcul de la note globale.

Détails de la note

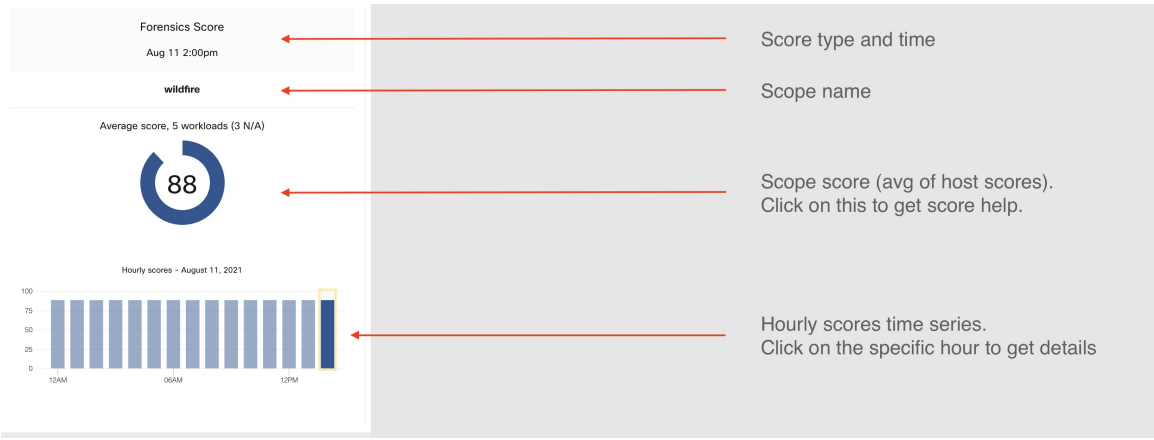
Chacune des six catégories suit le modèle suivant. Ce modèle présente la répartition des notes de la charge de travail, des séries chronologiques horaires et la distribution des notes de la portée enfant.



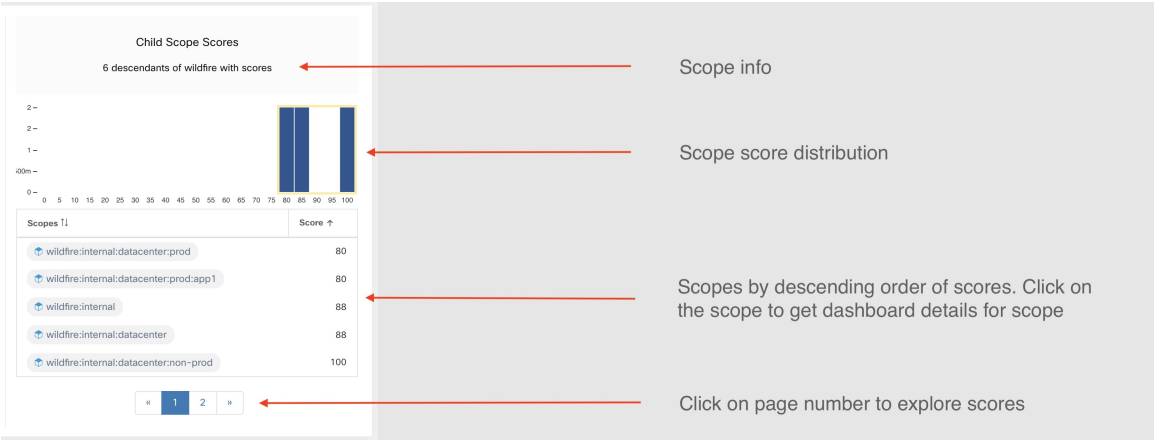
La répartition des notes des charges de travail fournit des indications sur la contribution aux notes des charges de travail dans le cadre de la portée sélectionnée. Il permet de faire ressortir les charges de travail les moins performantes pour accélérer les mesures correctives.



Les séries chronologiques horaires permettent d'obtenir le résultat horaire au cours d'une journée donnée. La sélection d'une heure dans la série chronologique met à jour la répartition des notes de la charge de travail et la répartition de la portée descendante afin d'afficher l'heure sélectionnée.



La répartition des portées descendantes fournit des informations sur la contribution au score des portées enfants de la portée sélectionnée.

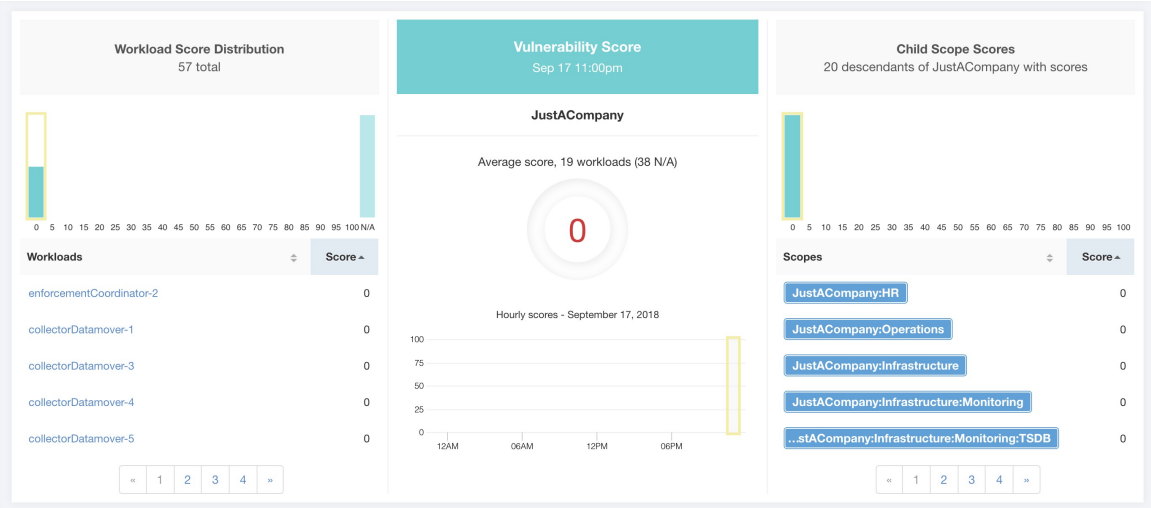


Les détails de chaque catégorie de note sont expliqués dans cette section.

Note de sécurité des vulnérabilités

Les vulnérabilités des paquets logiciels installés sur les charges de travail sont utilisées pour calculer la note de sécurité et de vulnérabilité.

Figure 519: Détails de la note de sécurité liée à la vulnérabilité



La note la plus faible indique :

- Un ou plusieurs paquets logiciels installés présentent de graves vulnérabilités.
- Appliquer un correctif ou une mise à niveau pour réduire les risques d'expositions ou d'exploits

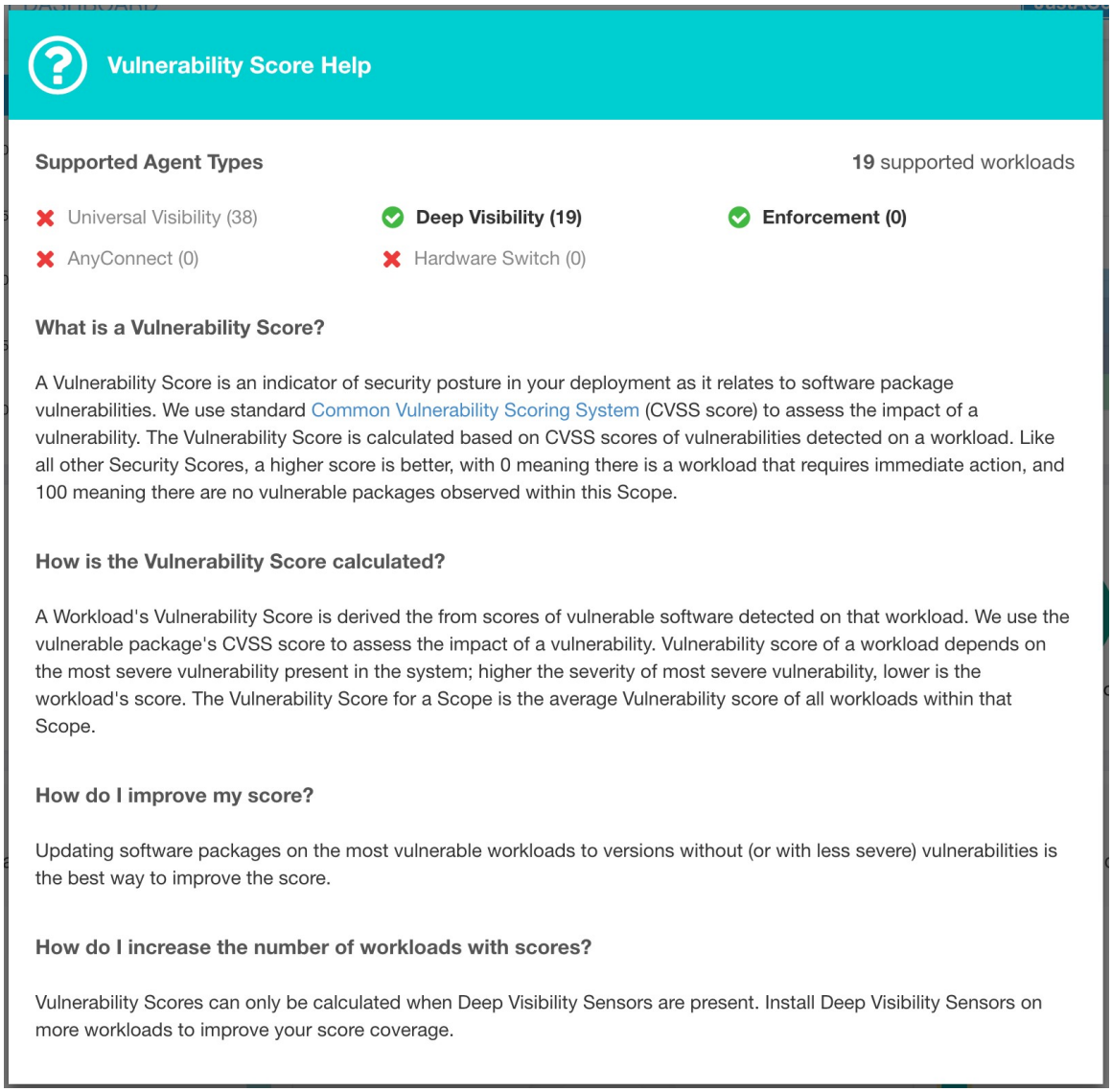
Les paquets logiciels sur les charges de travail pourraient être associés à des vulnérabilités connues (CVE). Le système CVSS (Common Vulnerability Scoring System) est utilisé pour évaluer l'impact d'une CVE. La plage de résultats CVSS va de 0 à 10, 10 étant la plus élevée.

Une CVE peut avoir une note CVSS v2 et CVSS v3. Pour calculer la note de vulnérabilité, CVSS v3 est pris en compte s'il est disponible, sinon CVSS v2 est pris en compte.

La note de vulnérabilité pour une charge de travail est dérivée des notes des logiciels vulnérables détectés sur cette charge de travail. La note de vulnérabilité de la charge de travail est calculée en fonction des résultats CVSS et des données des fournisseurs, et peut être ajustée par notre équipe de recherche sur la sécurité lorsque les données sont manquantes ou inexactes (ce qui est courant pour les nouvelles vulnérabilités). Ces données sont mises à jour toutes les 24 heures lors de la configuration du flux des menaces. Plus la gravité de la vulnérabilité la plus grave est élevée, plus la note est faible.

La note de portée est la moyenne des notes de charge de travail de la portée. Améliorez la note en identifiant les charges de travail ou les portées comportant des paquets logiciels vulnérables, et en appliquant des correctifs ou des mises à niveau avec des paquets plus sûrs.

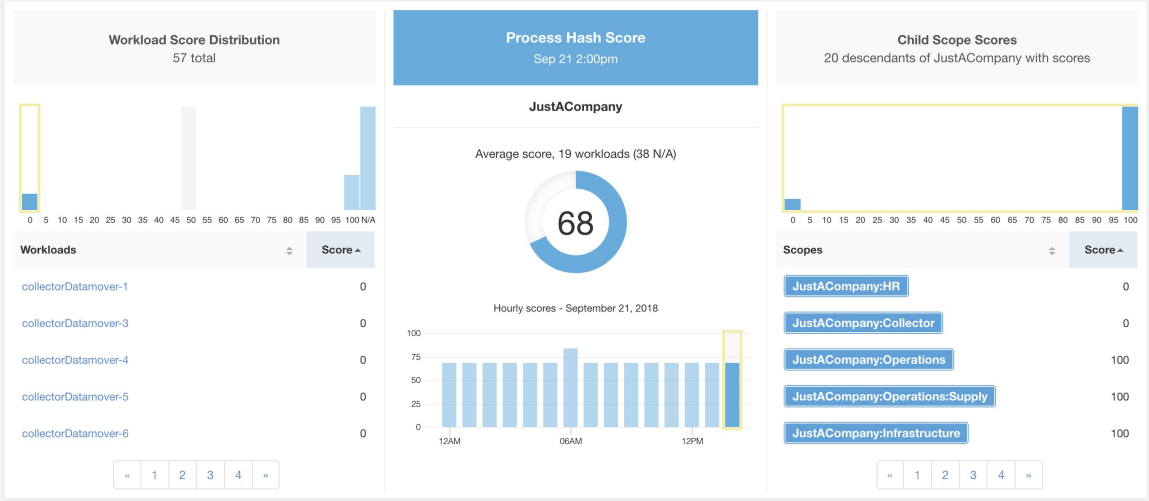
Figure 520: Aide sur la vulnérabilité et la note de sécurité



Note de condensé de processus

La note de condensé de processus est une évaluation de la cohérence du condensé binaire du processus (condensé de fichier) dans l'ensemble des charges de travail. Par exemple, une batterie de serveurs Web exécutant Apache qui est clonée à partir de la même configuration d'installation doit avoir le même condensé pour les fichiers binaires httpd sur tous les serveurs. Une incohérence est une anomalie.

Figure 521: Détails de la note de condensé de processus

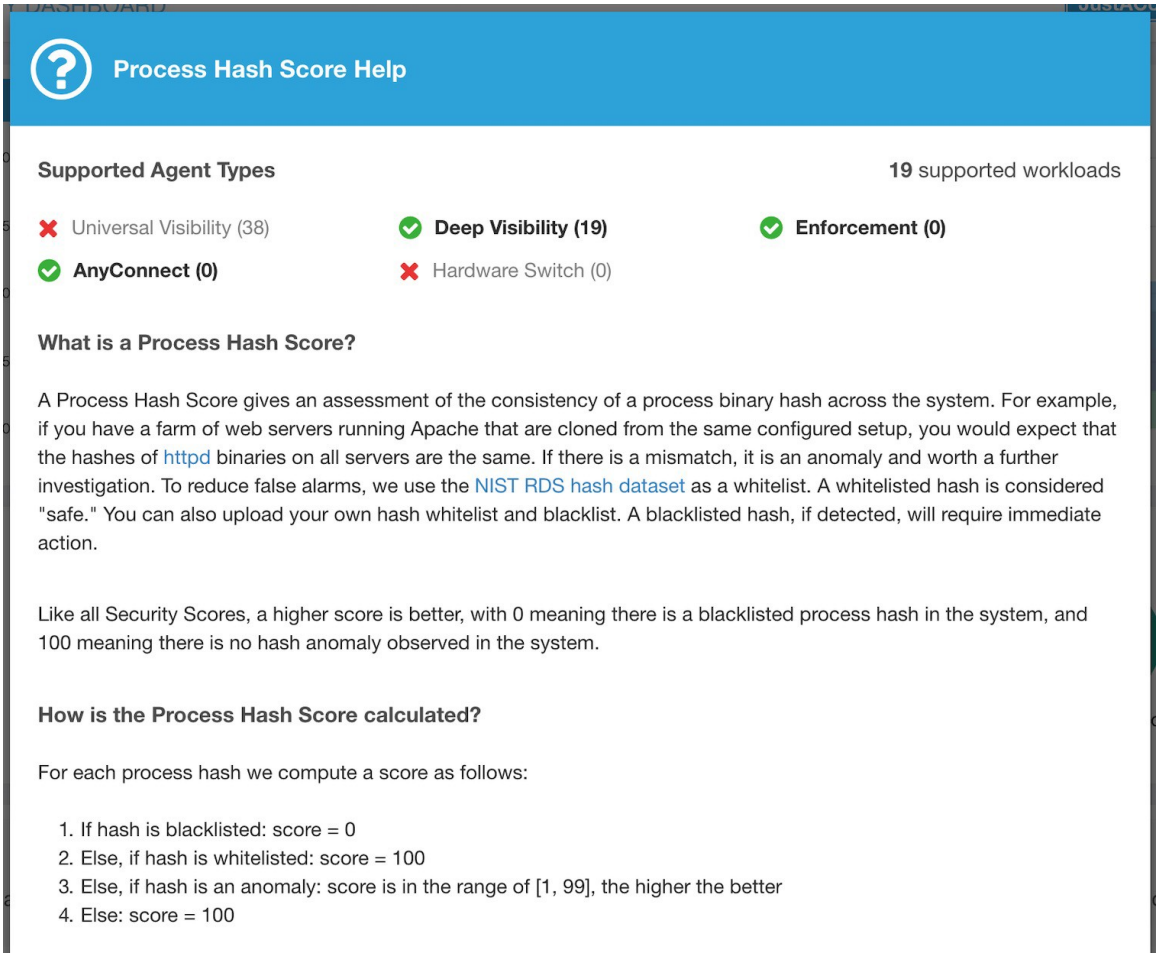


Une note plus basse indique qu'au moins l'un des éléments suivants, ou les deux, sont présents :

- Un ou plusieurs condensés de processus sont marqués par un indicateur.
- Un ou plusieurs condensés de processus sont anormaux.

Reportez-vous à la section Process hash anomaly detection pour plus de détails.

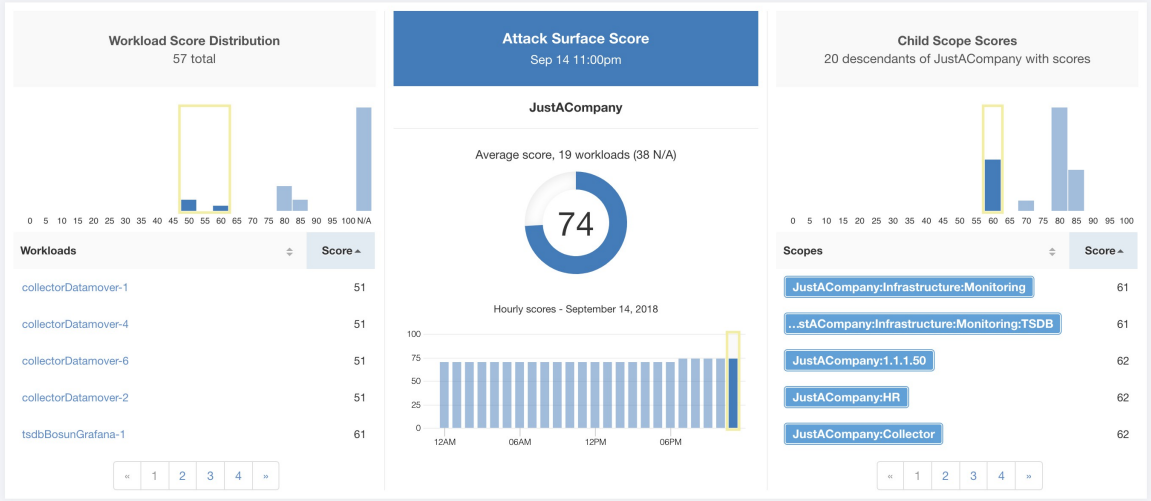
Figure 522: Aide sur la note de condensé de processus



Note de surface d'attaque

La note de surface d’attaque met en évidence la surface d’attaque potentielle dans une charge de travail. Les ports ouverts inutilisés (ports ouverts sans trafic) contribuent à abaisser ce score.

Figure 523: Détails de la note de surface d'attaque



Une note inférieure indique :

- De nombreux ports ouverts sans trafic au cours des 2 dernières semaines
- Des ports d'attaque bien connus peuvent être ouverts et inutilisés au cours des 2 dernières semaines.
- Un ou plusieurs ports ouverts sont associés à des paquets qui présentent de graves vulnérabilités.

La note de surface d'attaque est en fonction des ports ouverts inutilisés par rapport au nombre total de ports, avec un facteur de lissage. Les ports ouverts sans trafic au cours des deux dernières semaines sont considérés comme des « ports ouverts inutilisés ». Une pénalité supplémentaire est appliquée aux ports ouverts inutilisés qui sont des ports bien connus qui sont utilisés dans des attaques (par exemple, 21, 22, 8080, etc.).

Figure 524: Formule de la note de surface d'attaque

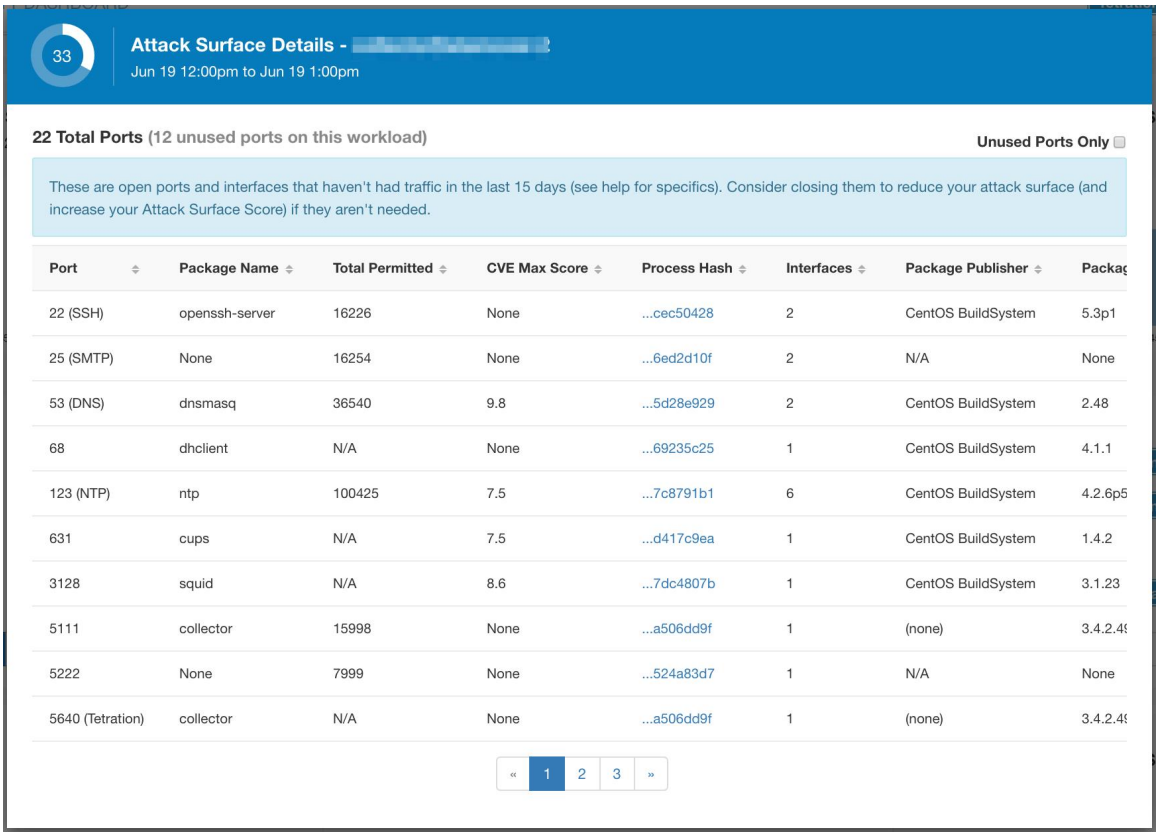
$$Attack\ surface\ score = \frac{\alpha + \sum used\ open\ ports}{\alpha + \sum open\ ports + (\rho * \sum unused\ common\ attack\ ports\ ) + f_v(vulnerablity\ pkgs)}$$

$$f_v = \max\left(\left\{cve_{score} = \begin{cases} CVSS_{V3}, & v3\ exist \\ CVSS_{V2}, & v3\ not\ exist \end{cases}\right\}\right)$$

Le lissage de Laplace est utilisé avec un facteur de pénalité basé sur des données heuristiques. La note est calculée quotidiennement avec les deux dernières semaines de données.

La note du détenteur est la moyenne des notes de la charge de travail de la portée. Améliorer le score en identifiant la charge de travail ou les portées avec des ports ouverts inutilisés, et en fermant les ports inutilisés.

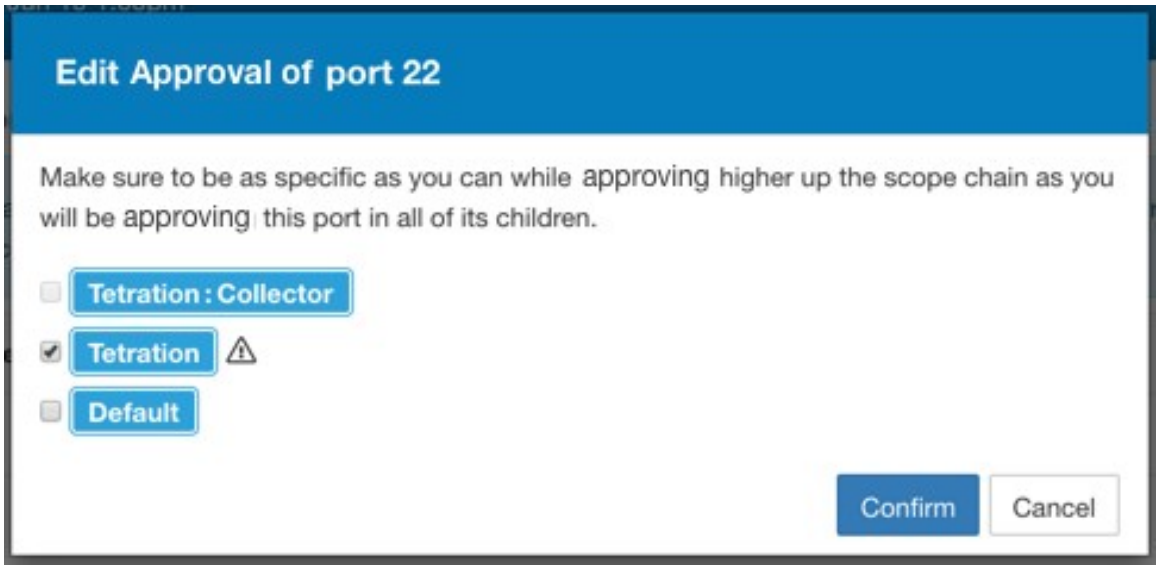
Lorsque vous cliquez sur le lien d'une charge de travail, une boîte de dialogue modale de surface d'attaque est ouverte avec des détails sur tous les ports et toutes les interfaces disponibles dans le contexte de cette charge de travail.



Caractéristiques :

- Ports inutilisés uniquement : cochez cette case lorsque cette option filtre les ports utilisés et affiche uniquement les ports inutilisés associés à la charge de travail.
- Colonnes : approuvé, port, nom du paquet, total autorisé, note CVE maximale, condensé de processus, interfaces, serveur de publication du paquet, version du paquet, total échappé, total rejeté, ports couramment piratés, liens.
- Interfaces : Si vous cliquez sur l'un des éléments de ligne du tableau Surface d'attaque, vous pouvez afficher les interfaces associées à chaque port dans une boîte de dialogue modale.
- Approuvé : case à cocher, lorsqu'elle est cochée, vous permet de définir intentionnellement un « port inutilisé » comme « approuvé » sur l'un des champs de la chaîne de portées à laquelle cette charge de travail a accès. Remarque : si un port est approuvé pour une portée et que ce port n'est explicitement approuvé sur aucune des portées enfants (si cette portée a des enfants), les cases de la portée sont désactivées, car il est implicite que toute portée enfant à laquelle la portée parente a accès à est déjà approuvé dans cette chaîne.

Boîte de dialogue modale d'approbation :



Boîte de dialogue modale des interfaces :

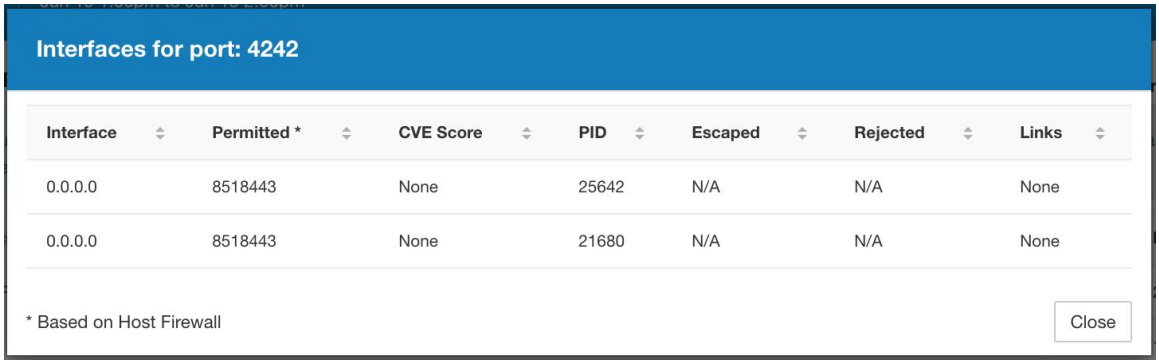
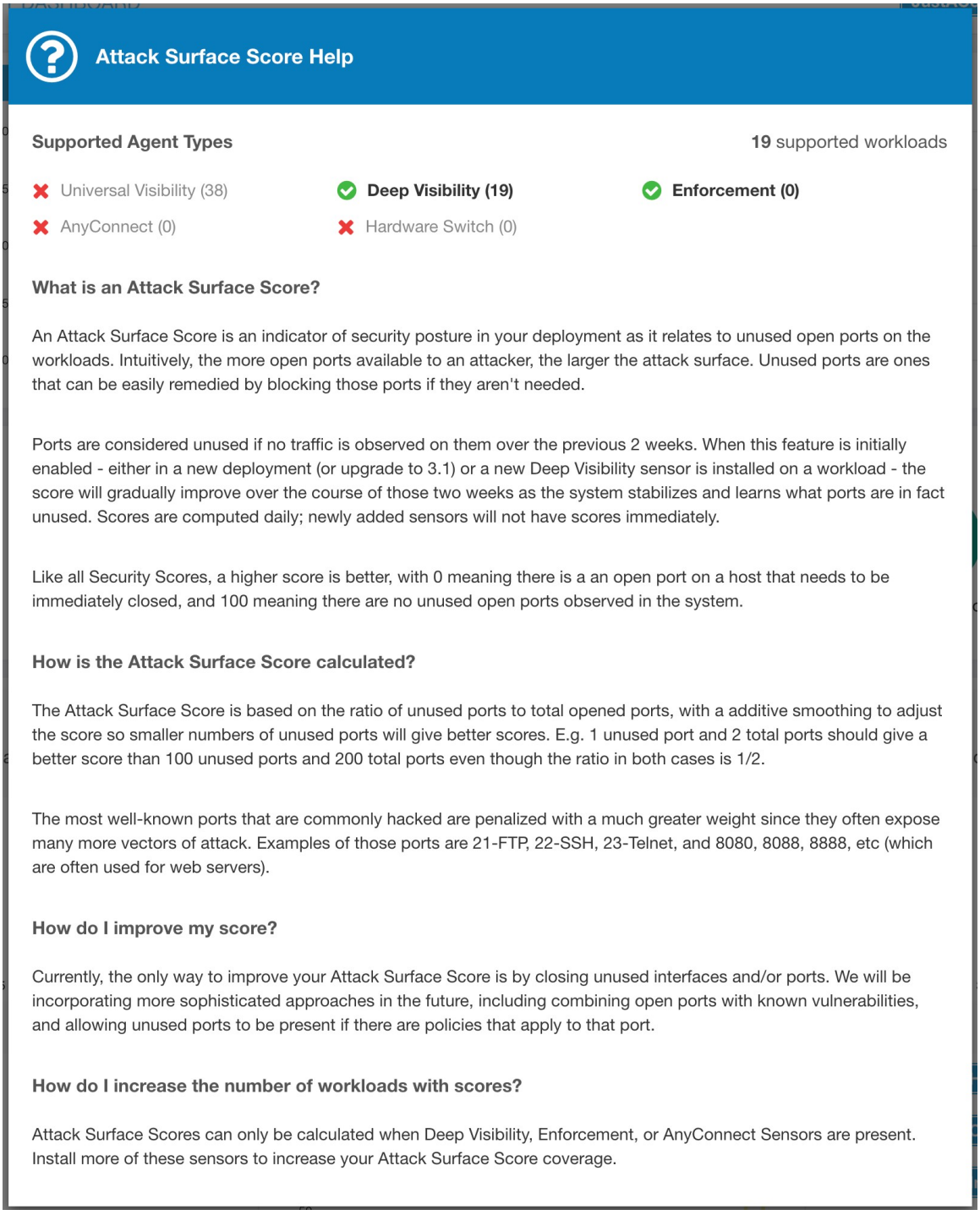


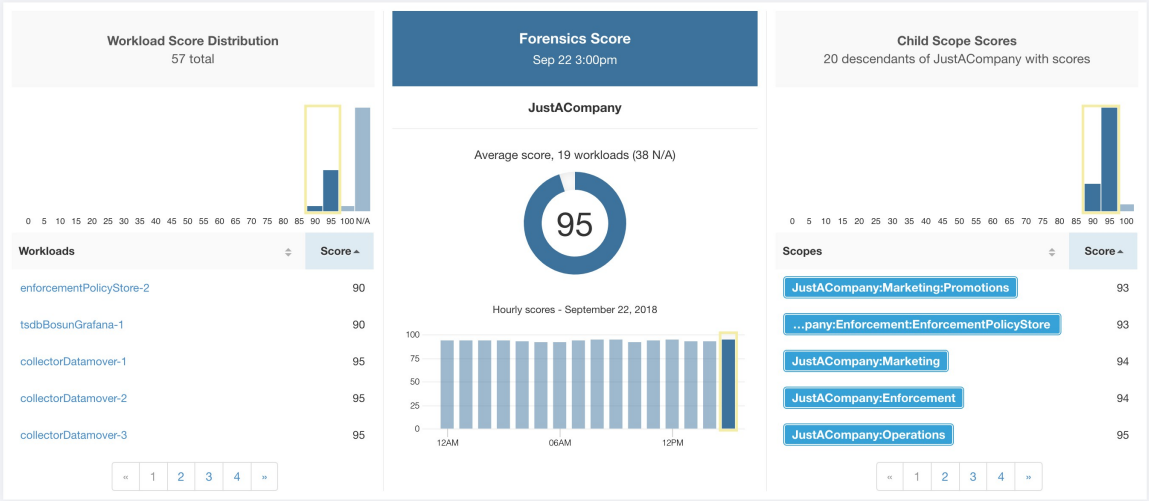
Figure 525: Aide sur la note de surface d'attaque



Note de criminalistique

La gravité des événements criminalistiques sur les charges de travail est utilisée pour calculer les notes.

Figure 526: Détails de la note criminalistique



La note la plus faible indique :

- Un ou plusieurs événements criminalistiques ont été observés sur la charge de travail.
- Ou une ou plusieurs règles criminalistiques sont parasitées ou incorrectes.

Pour améliorer le résultat :

- Corrigez le problème, le cas échéant, pour réduire les risques d'expositions ou d'exploitations.
- Ajustez les règles criminalistiques pour réduire le bruit et les fausses alertes.

La note criminalistique pour une charge de travail est inversement proportionnelle à la note d'impact totale des événements criminalistiques. Plus la note d'incidence totale des événements criminalistiques est élevée, plus leur incidence est faible.

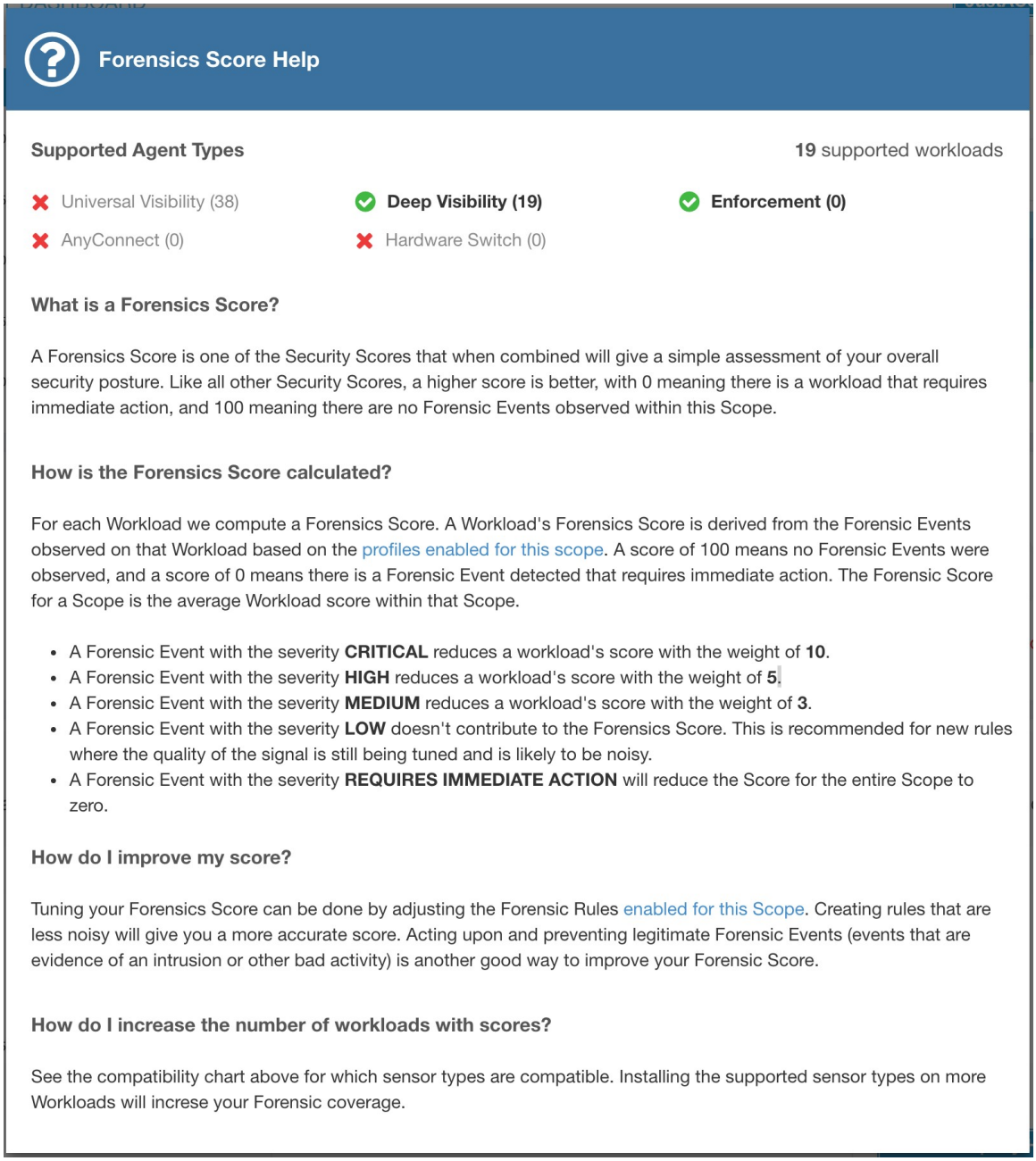
Gravité	Note d'incidence
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	100
CRITIQUE	10
ÉLEVÉE	5
CRITIQUE	3

Figure 527: Formule de note criminalistique

$$forensics\ score = max\left(0, (100 - \sum forensics\ event\ impact\ score)\right)$$

Reportez-vous à la section Configurer et surveiller les événements criminalistiques pour plus de détails.

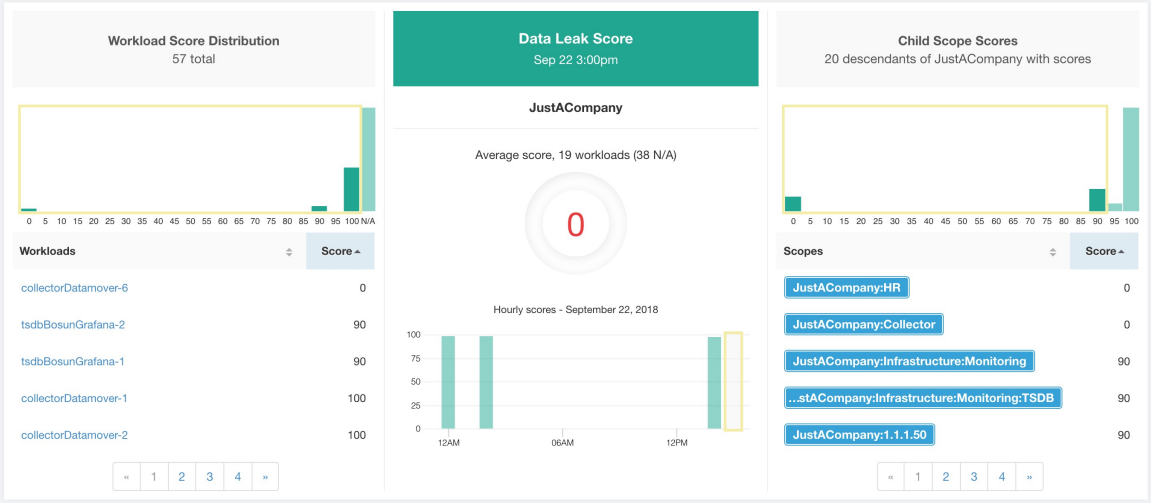
Figure 528: Aide relative à la note criminalistique



Note d'anomalie de réseau

La gravité des événements d'anomalie de réseau sur les charges de travail est utilisée pour calculer les notes.

Figure 529: Détails de la note de fuite de données



La note la plus faible indique :

- Une quantité inhabituellement élevée de données est transférée à partir des charges de travail.
- Ou la règle criminalistique d'anomalie de réseau est incorrecte ou parasitée par du bruit.

Pour améliorer le résultat :

- Corrigez le problème, le cas échéant, pour réduire les risques d'exfiltration de données.
- Ajustez les règles d'anomalies de réseau pour réduire le bruit et les fausses alertes.

La note d'anomalie de réseau pour une charge de travail est inversement proportionnelle à la note de gravité totale des événements d'anomalie de réseau. Plus la note d'anomalie totale de réseau est élevée, plus la note d'anomalie de réseau est faible.

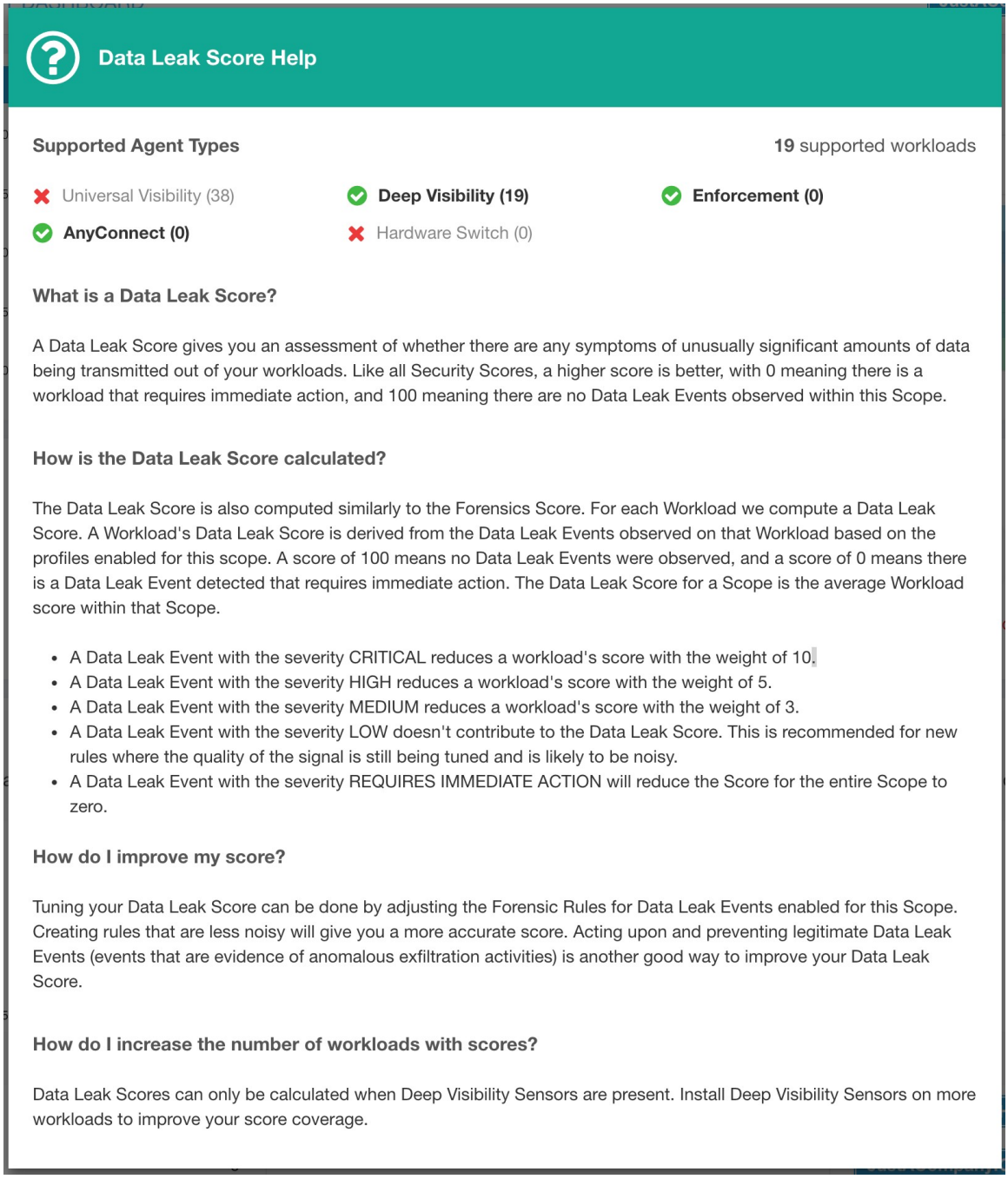
Gravité	Résultat
IMMEDIATE_ACTION (ACTION_IMMÉDIATE)	100
CRITIQUE	10
ÉLEVÉE	5
CRITIQUE	3

Figure 530: Formule de la note de fuite de données

$$data\ leak\ score = max\left(0, (100 - \sum data\ leak\ event\ severity\ score)\right)$$

Reportez-vous à la section Détection des anomalies de réseau basée sur le PCR pour en savoir plus.

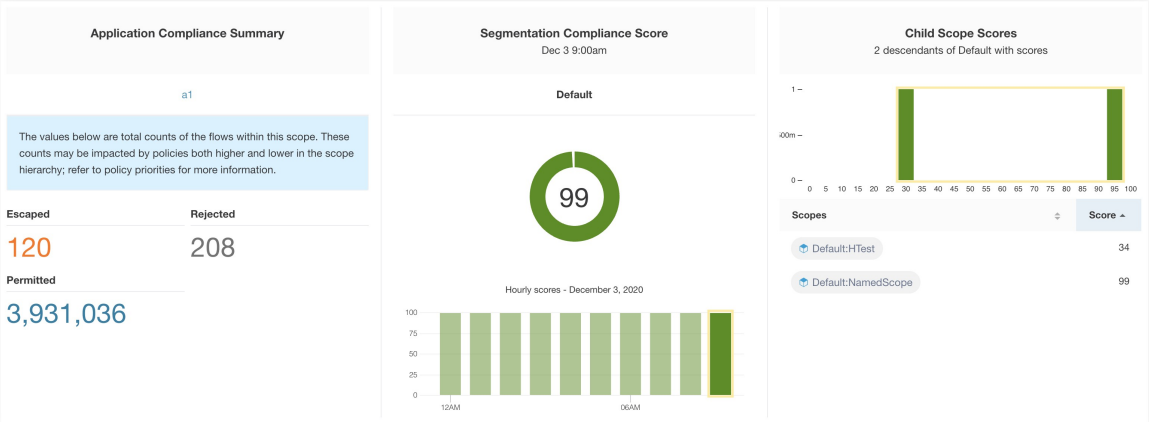
Figure 531: Aide sur la note de fuite de données



Note de conformité de la segmentation

La note de conformité de la segmentation présente une vue générale des violations de politique et souligne les portées et les espaces de travail qui ont subi le plus grand nombre de violations.

Figure 532: Détails de la note de conformité de la segmentation



Note Le nombre d'échappés, de refus ou d'autorisations affiché dans le tableau de bord de sécurité pour la portée racine ne correspond pas à tous les nombres affichés respectivement pour toutes les portées enfants. Le nombre d'échappés, de refus ou d'autorisations est une évaluation de la politique et pas seulement de la source ou de la destination.

La note la plus faible indique :

- Nombre important de flux échappés (violations de politique) par rapport à la valeur autorisée
- La note est de 0 lorsqu'il y a plus de flux échappés que celui autorisé.

La note de conformité de la segmentation est calculée pour les portées avec un espace de travail principal appliqué. Pour les portées sans espaces de travail appliqués, la note sera calculée comme la moyenne des notes des portées descendantes comportant des politiques appliquées.

La note est calculée en utilisant le rapport entre échappé et autorisé.

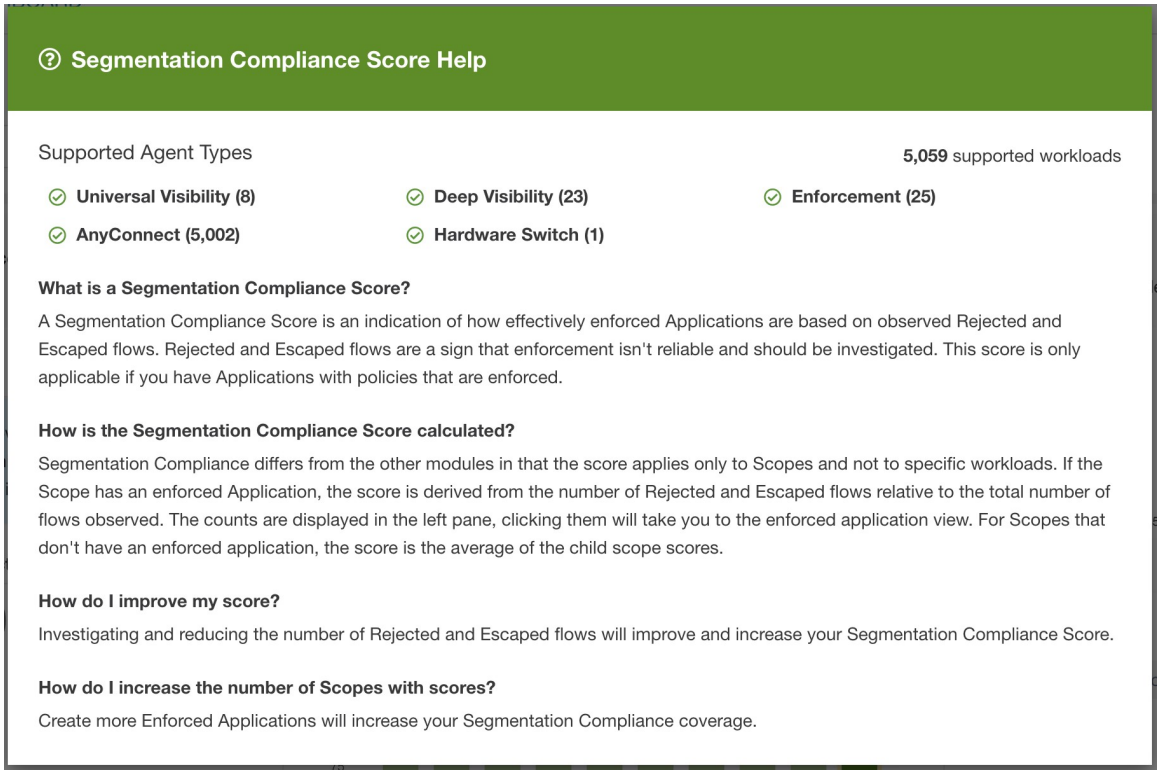
Figure 533: Formule de la note de conformité de la segmentation

$$compliance\ score = \left\lfloor 100 - \frac{100 \times escaped}{permitted} \right\rfloor$$

Améliorer le score en réduisant le nombre de violations de politique

- Vérifiez que les politiques couvrent correctement le comportement souhaité.
- Vérifiez que les politiques sont correctement appliquées.

Figure 534: Aide pour les détails sur le niveau de conformité de la segmentation



CHAPITRE 16

Afficher le tableau de bord des vulnérabilités

Le tableau de bord des vulnérabilités permet aux utilisateurs finaux de concentrer leurs efforts sur les vulnérabilités critiques et les charges de travail qui nécessitent le plus d'attention. Vous pouvez sélectionner la portée appropriée en haut de cette page et sélectionner le système de notation pour les vulnérabilités que vous souhaitez afficher (Common Vulnerability Scoring System v2 ou v3). La nouvelle page met en évidence la répartition des vulnérabilités dans la portée choisie et affiche les vulnérabilités selon différents attributs, par exemple, la complexité des exploits, les vulnérabilités peuvent-elles être exploitées sur le réseau ou l'attaquant a-t-il besoin d'un accès local à la charge de travail. De plus, des statistiques permettent de filtrer rapidement les vulnérabilités exploitables à distance et les plus complexes à exploiter.

Tableau de bord des vulnérabilités

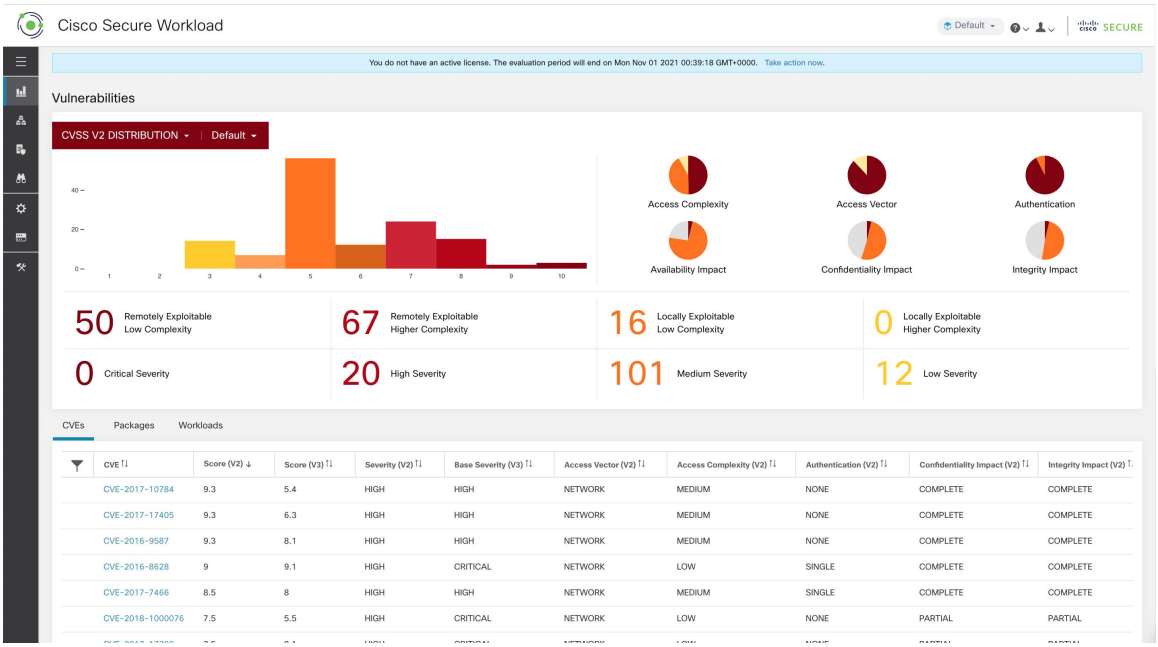
Trois onglets sont disponibles dans le tableau de bord des vulnérabilités. Ils sont tous ajustés ou filtrés en fonction des clics des utilisateurs sur les gadgets en haut de la page :

- L'onglet des CVE met en évidence les vulnérabilités sur lesquelles il faut se concentrer au sein de la portée choisie.
- L'onglet Paquets montre aux utilisateurs finaux les paquets qui doivent être corrigés.
- L'onglet Charges de travail répertorie les charges de travail qui nécessitent le plus d'attention en termes d'applications de correctifs dans la portée choisie.

Cliquez sur n'importe quelle ligne des onglets ci-dessus pour en savoir plus à ce sujet. Par exemple, cliquez sur la ligne du paquet dans l'onglet des paquets pour afficher les charges de travail sur lesquelles ce paquet ou cette version est installée et les vulnérabilités associées à ce paquet. De même, cliquez sur une ligne dans l'onglet des charges de travail pour afficher les paquets installés sur la charge de travail choisie ainsi que les vulnérabilités associées.

Cette page est destinée à aider les utilisateurs à identifier les charges de travail sur lesquelles se concentrer en premier et les paquets à corriger en premier.

Figure 535: Tableau de bord des vulnérabilités



Pour afficher le tableau de bord des vulnérabilités, dans le volet de navigation, choisissez **Investigate (Enquêter)** > **Vulnerabilities (Vulnérabilités)**.

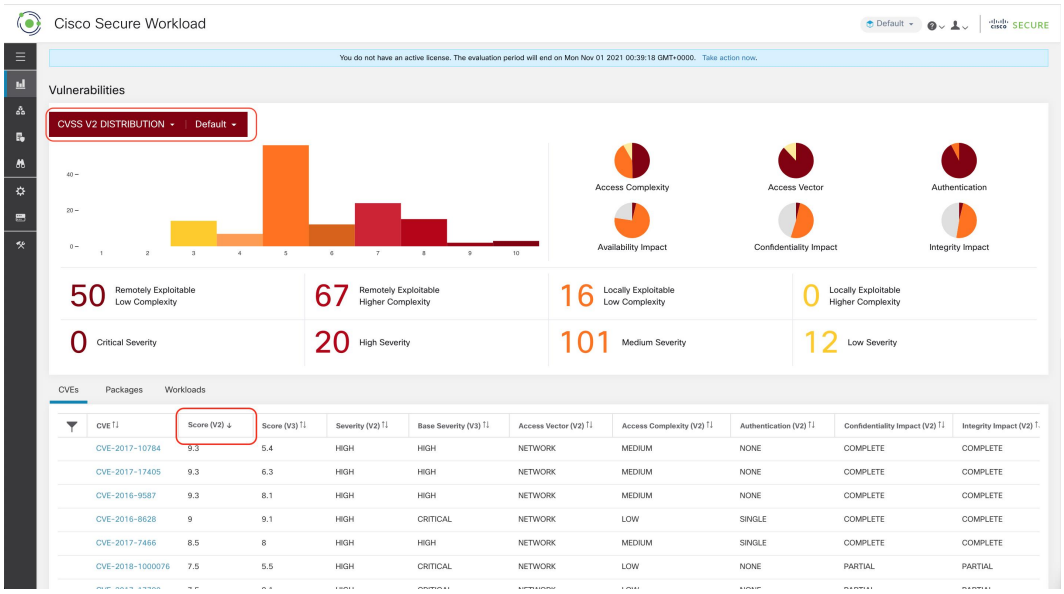
Onglet CVE

En fonction de la portée sélectionnée dans le haut de la page et du système de notation (v2 ou v3), l'onglet CVE met en évidence les vulnérabilités (triées par les niveaux) dans les charges de travail des portées sélectionnés qui nécessitent une attention.

Pour chaque CVE, en plus des mesures d'impact de base, des informations sur les exploits basées sur nos informations sur les menaces sont affichées :

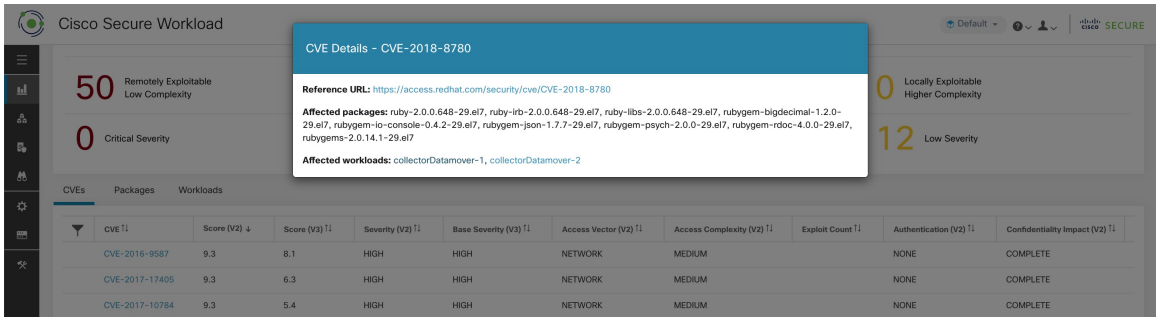
- Nombre d'exploits : nombre de fois où la CVE a été constatée exploitée de manière incontrôlée au cours de l'année écoulée.
- Dernier exploit : la dernière fois que l'exploitation de la CVE de manière incontrôlée a été constatée par nos services de renseignement sur les menaces.

Figure 536: Onglet des CVE répertoriant les vulnérabilités dans une portée spécifiée



Cliquez sur une ligne du tableau des CVE pour obtenir plus de détails sur cette vulnérabilité et les charges de travail qu'elle affecte.

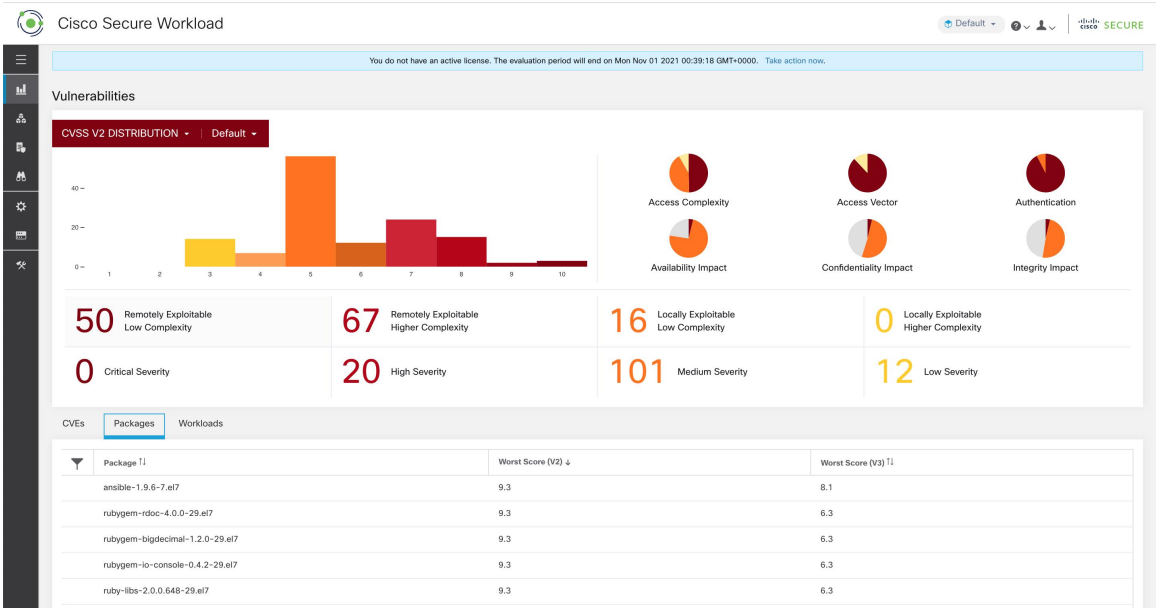
Figure 537: Détails d'une CVE



Onglet Packages (Logiciels)

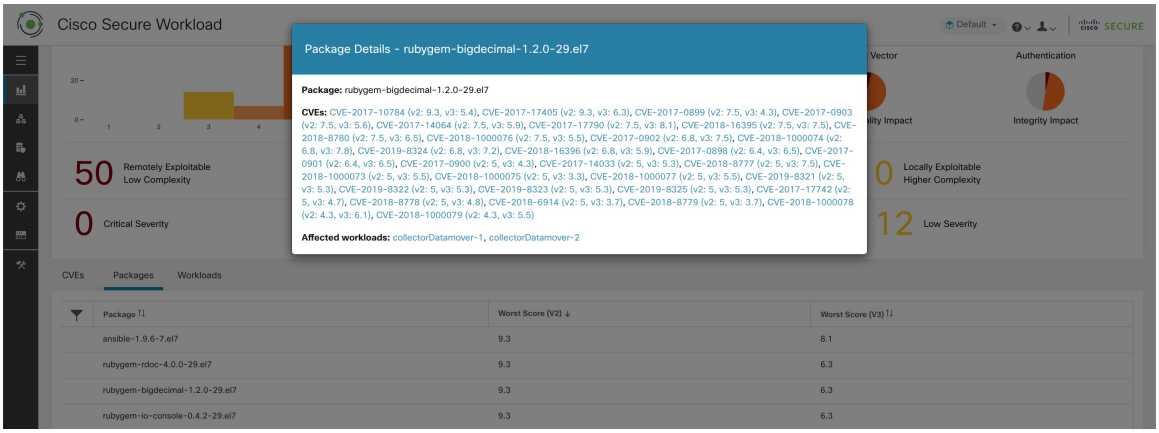
L'onglet Packages (Logiciels) répertorie les progiciels auxquels les utilisateurs doivent prêter attention et qui doivent éventuellement être mis à niveau pour réduire leur surface d'attaque.

Figure 538: Onglet Packages (Logiciels) répertoriant les logiciels vulnérables dans une portée spécifiée



En cliquant sur une ligne du tableau des paquets logiciels, vous obtiendrez plus de détails sur les charges de travail pour lesquelles le paquet est installé, ainsi que sur les CVE connus pour ce paquet.

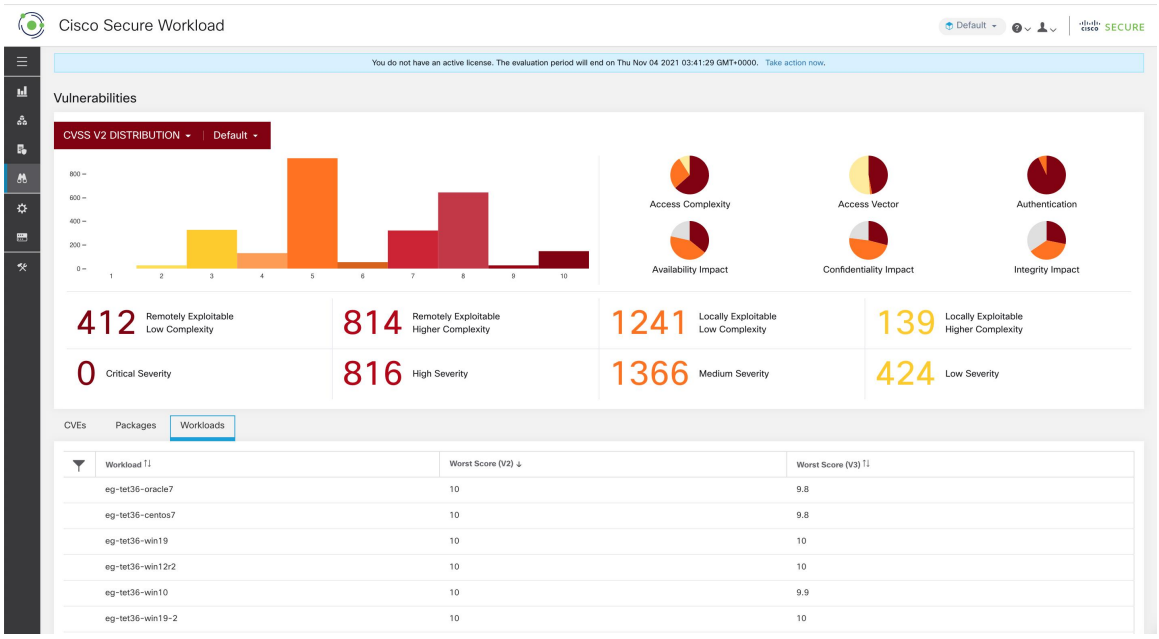
Figure 539: Détails des vulnérabilités et des charges de travail concernées pour un paquet



Onglet Charges de travail

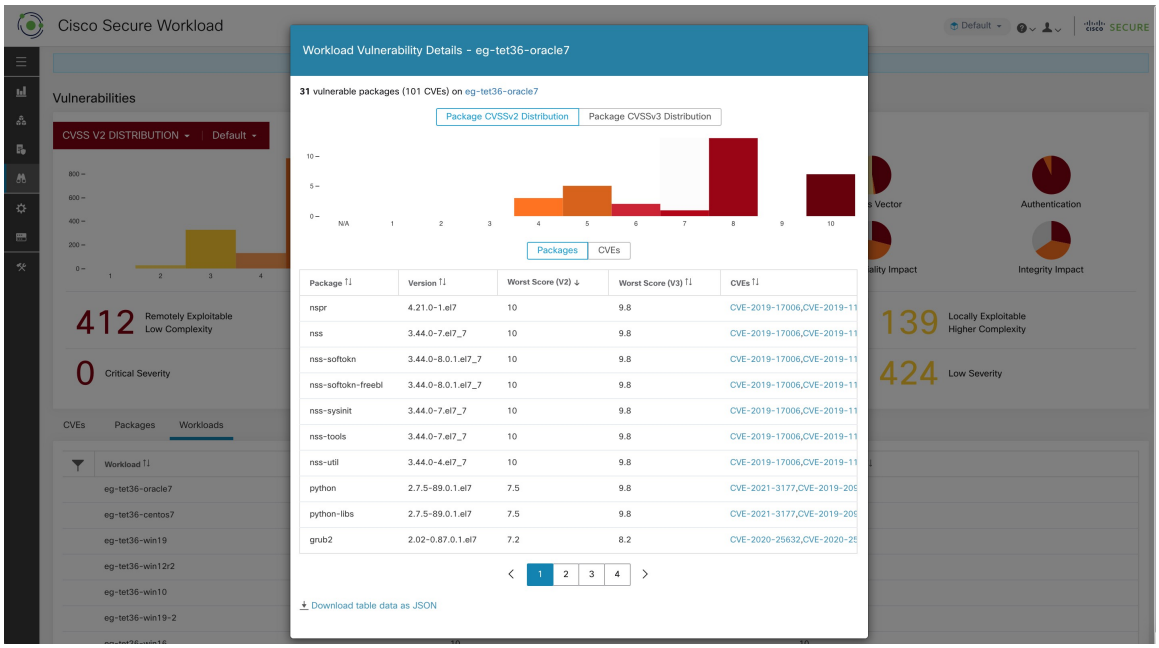
L'onglet Charges de travail répertorie les charges de travail qui nécessitent votre attention en termes de mises à jour logicielles ou de correctifs.

Figure 540: Onglet Charges de travail répertoriant les charges de travail vulnérables dans la portée spécifiée



Cliquez sur une ligne du tableau des charges de travail pour obtenir la liste des paquets avec des vulnérabilités sur cette charge de travail.

Figure 541: Détails des vulnérabilités pour une charge de travail



Tous les tableaux ci-dessus peuvent être téléchargés en utilisant les liens de téléchargement au bas des tableaux.

CHAPITRE 17

Effectuer les configurations de système dans Cisco Secure Workload

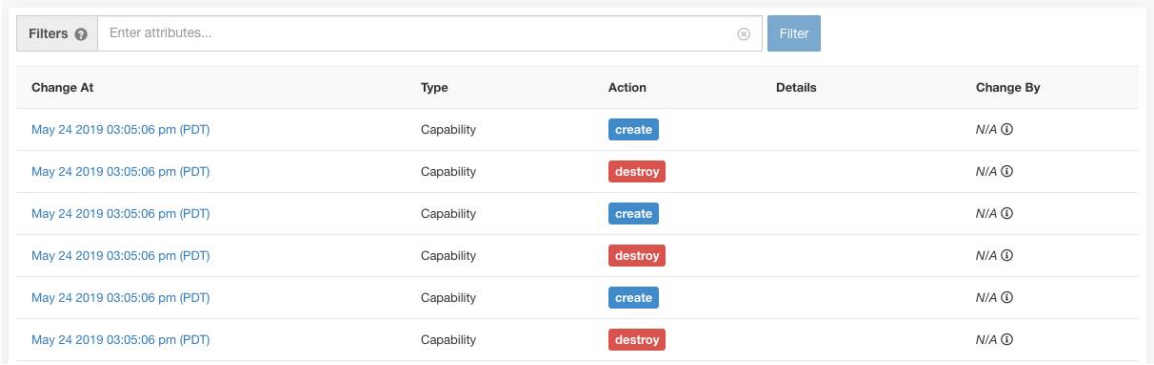
Les paramètres au niveau du système sont à votre disposition en fonction de votre rôle. Par exemple, seuls les utilisateurs ayant le rôle d' **administrateur de site** et de **service d'assistance à la clientèle** peuvent afficher l'option **Users** (Utilisateurs).

Journal des modifications

Les **administrateurs du site** peuvent accéder à la page **Change Log**(Journal des modifications) dans le menu **Manage** (Gérer) dans la barre de navigation à gauche de la fenêtre. Cette page affiche les modifications les plus récentes effectuées dans Cisco Cisco Secure Workload.

Note **Période de rétention des journaux des modifications** : Cisco Secure Workload gère les journaux des modifications pour une durée maximale d'un an sur les grappes de logiciels-services et sur site. Une tâche horaire supprime les journaux des modifications qui dépassent une période d'un an.

Figure 542: Page du journal des modifications

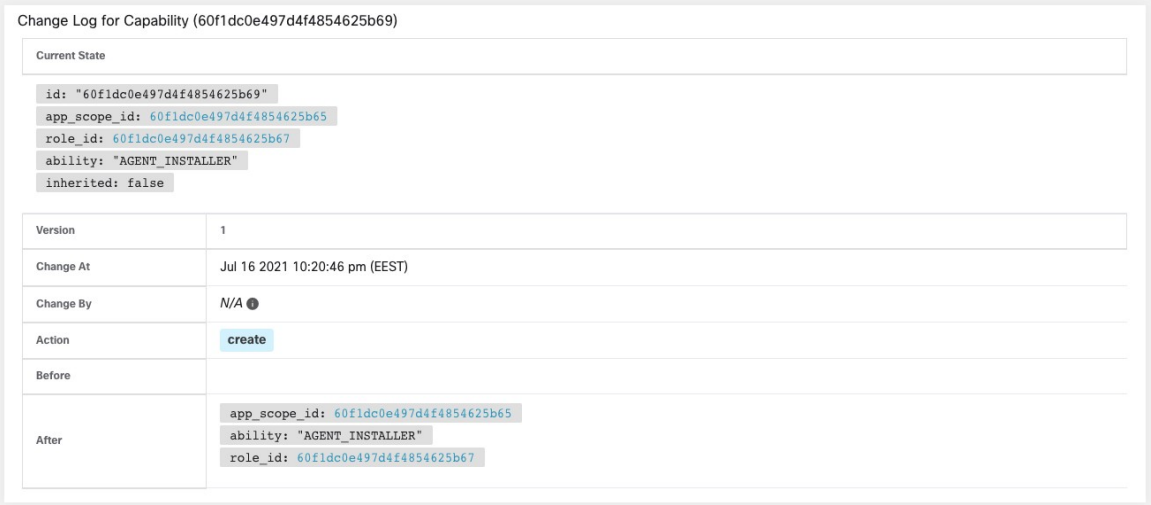


Pour consulter les détails de chaque entrée du journal des modifications, cliquez sur le lien dans la colonne **Change at** (Modifier à). Cette page comprend un instantané **avant** et **après** des champs modifiés. Les champs peuvent inclure des noms techniques qui nécessitent une certaine interprétation pour comprendre comment ils sont présentés ailleurs dans Cisco Secure Workload.

Figure 543: Page des détails du journal des modifications

La liste complète des modifications pour une entité peut être consultée en cliquant sur le bouton dans le coin supérieur droit, intitulé **Full log for this <entity type>** (Journal complet pour ce <type d'entité>). Cette page affiche les détails de chaque modification. Elle comprend également l' **état actuel** de l'entité, lorsqu'il est disponible.

Figure 544: Journal complet des modifications pour l'entité



Règles de collecte

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Collection Rules** (règles de collecte) dans le menu **Manage (Gestion) > Services Settings(Paramètres de service)** dans la barre de navigation à gauche de la fenêtre. Cette page affiche les règles de collecte matérielles par VRF qui sont utilisées par les commutateurs exécutant l'agent Cisco Cisco Secure Workload. Il y a une ligne dans le tableau pour chaque VRF.

Règles

Cliquez sur le bouton **Edit** (modifier) d'un VRF pour modifier ses règles de collecte. Par défaut, chaque VRF est configuré avec deux règles collecteurs par défaut, une pour IPv4 `(0.0.0.0/0 INCLUDE)` et une pour IPv6 `(::/0 INCLUDE)`. *Ces règles par défaut peuvent être supprimées, mais procédez avec prudence.*

Des règles d'inclusion et d'exclusion supplémentaires peuvent être ajoutées. Saisissez un sous-réseau valide, sélectionnez inclure ou exclure, puis cliquez sur **Add Rule** (Ajouter une règle). La priorité de ces règles peut être ajustée par glisser-déposer. Cliquez et maintenez une règle dans la liste et faites-la glisser pour ajuster l'ordre.

Plusieurs minutes peuvent être nécessaires pour que les modifications se propagent à vos commutateurs. Cliquez sur le bouton **Back** (Précédent) dans le coin supérieur droit pour revenir à la liste des fichiers VRF.

Priority (priorité)

Les règles de collecte sont classées par ordre de priorité décroissant. Aucune correspondance du préfixe le plus long n'est effectuée pour déterminer la priorité. La règle apparaissant en premier a une priorité plus élevée sur toutes les règles suivantes. Exemple :

1. 1.1.0.0/16 INCLUDE
2. 1.0.0.0/8 EXCLUDE

3. 0.0.0.0/0 INCLUDE

Dans l'exemple précédent, toutes les adresses appartenant au sous-réseau 1.0.0.0/8 sont exclues, sauf le sous-réseau 1.1.0.0/16 qui est inclus.

Autre exemple avec ordre modifié :

1. 1.0.0.0/8 EXCLUDE
2. 1.1.0.0/16 INCLUDE
3. 0.0.0.0/0 INCLUDE

Dans l'exemple ci-dessus, toutes les adresses appartenant au sous-réseau 1.0.0.0/8 sont exclues. La règle numéro 2 n'est pas appliquée ici, en raison d'une règle d'ordre supérieur déjà définie pour son sous-réseau.

Collecteurs

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Collectors** (Collecteurs) dans le menu **Platform** (Plateforme) dans la barre de navigation à gauche de la fenêtre. Cette page affiche les collecteurs actuellement configurés. Les agents Cisco Secure Workload envoient des données de flux aux collecteurs mis en service. Il est donc important que tous les collecteurs mis en service soient disponibles. Par défaut, l'intégrité de tous les collecteurs fait l'objet d'une vérification périodique et ils sont mis en service ou désactivés en fonction de leur intégrité. Vous pouvez vous désinscrire de ce processus automatisé en utilisant le bouton **Auto Commission Opt Out** (pour la désactivation automatique de la commission). Lorsque cette bascule est activée, les icônes **Play** (Lecture) et **Stop** (Arrêt) sous la colonne la plus à droite peuvent être utilisées pour la mise en service et la désactivation respectivement.

Figure 545: Page Collectors (Collecteurs)

Configuration de session

Le délai d'expiration de la session d'inactivité de l'authentification de l'utilisateur de l'interface utilisateur peut être configuré ici. Cette configuration s'applique à tous les utilisateurs de l'appareil. La durée par défaut d'une session inactive est de 1 heure. La durée d'une session d'inactivité peut être définie entre 5 minutes et 24 heures. Le délai d'expiration de session prend effet sur la session authentifiée d'un utilisateur lorsque cette valeur est enregistrée.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à ce paramètre. Dans le volet de navigation de gauche, cliquez sur **Manage (Gestion)** > **Service Settings(Paramètres de service)** > **Session Configuration (Configuration de la session)**.

Société

Vous pouvez définir les configurations suivantes à l'échelle de l'entreprise (par Cisco Secure Workload grappe ».

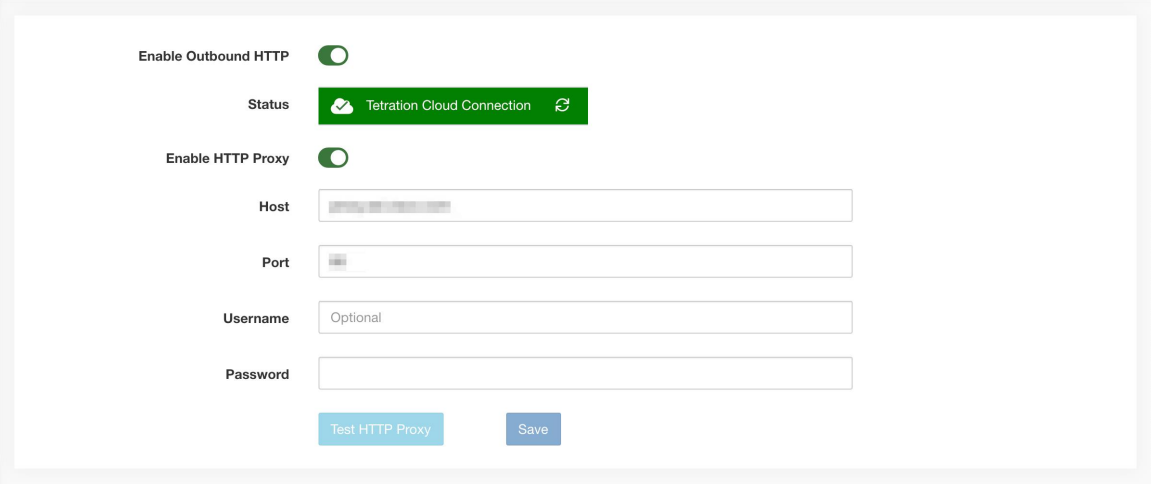
Connexion HTTP sortante

Pour vous assurer que les derniers ensembles de données d'informations sur les menaces sont récupérés à partir de Cisco Cloud, nous vous recommandons fortement de configurer une connexion HTTP sortante.

Warning Votre demande HTTP sortante d'entreprise peut nécessiter d'autoriser le trafic vers **periscope.tetrationcloud.com** et **uas.tetrationcloud.com** dans les règles de sortie du pare-feu d'entreprise en plus de configurer le serveur mandataire HTTP comme indiqué ci-dessous.

La connexion TLS à **periscope.tetrationcloud.com** est utilisée pour transporter des données d'informations sur les menaces afin d'identifier les vulnérabilités connues. Par conséquent, il est essentiel que Cisco Cisco Secure Workload vérifie l'authenticité du nom de domaine en comparant le certificat de l'autorité de certification x.509 du domaine par rapport aux certificats d'autorité de certification racine réputés inclus avec Cisco Secure Workload. L'altération de la chaîne de confiance X.509 empêche la fonctionnalité de fonctionner correctement.

Figure 546: Connexion HTTP sortante



Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder aux paramètres HTTP sortants. Dans la barre de navigation à gauche, cliquez sur **Platform(Plateforme)** > **Outbound HTTP (HTTP sortant)**.

Champ	Description
État	Indique si l'appareil Cisco Secure Workload peut accéder à Cisco Secure Workload infonuagique pour récupérer les mises à jour de l'ensemble de données des menaces. La vérification de l'état peut être redéclenchée en cliquant sur le bouton d'actualisation. Les paramètres de serveur mandataire HTTP suivants peuvent être utilisés pour configurer les paramètres de serveur mandataire HTTP en fonction de votre déploiement Cisco Secure Workload.

Champ	Description
Activer le serveur mandataire HTTP	Toutes les connexions HTTP externes utilisent un serveur mandataire HTTP si cette option est activée
Hébergement	Adresse de l'hôte du serveur mandataire HTTP
Port	Numéro de port du serveur mandataire HTTP
Nom d'utilisateur	Nécessaire uniquement si votre serveur mandataire HTTP utilise l'authentification de base
mot de passe	Nécessaire uniquement si votre serveur mandataire HTTP utilise l'authentification de base

Message de page de connexion

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent saisir un message de 1 600 caractères maximum que les utilisateurs peuvent voir sur la page de connexion.

Pour créer ou modifier le message de la page de connexion :

1. Dans la page de navigation de gauche, cliquez sur **Platform (Plateforme)** > **Login Page Message (Message de la page de connexion).**
2. Saisissez ou modifiez le message. La limite de caractères est inférieure ou égale à 1 600 caractères.
3. Cliquez sur **Save** (enregistrer).

Configurer l'authentification externe

Si cette option est activée, l'authentification peut être transférée à un système externe. Les options actuelles d'authentification sont le protocole LDAP (Lightweight Directory Access Protocol) et la connexion unique (Single Sign-On ou SSO). Cela signifie qu'une fois activé, tous les utilisateurs qui se connectent utiliseront le mécanisme choisi pour s'authentifier. Il est important d'établir que la connexion LDAP est configurée correctement, en particulier si aucun utilisateur ne recourt à l' option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale). L'approche recommandée est d'avoir au moins un utilisateur authentifié localement avec des informations d'authentification d' **Site Admin** (administrateur de site) en activant l'option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale). Cet utilisateur peut s'assurer que la configuration LDAP est configurée correctement. Une fois la connexion configurée, cet utilisateur peut également être transféré vers l'authentification externe en décochant l'option « Use Local Authentication » (Utiliser l'authentification locale) dans le flux de modification de l'utilisateur.

L'administrateur du site peut activer davantage de messages de débogage, ce qui est utile pour déboguer les problèmes de connexion externe, les échecs de connexion de l'utilisateur, etc. Ils peuvent être activés en cochant l'option « External Auth Debug » (Débogage de l'authentification externe). Une fois cette option activée, des messages de journalisation plus descriptifs sont écrits dans un fichier journal distinct intitulé « external_auth_debug.log » (journal_auth_debog_externe). Il est recommandé de désactiver le « débogage

d'authentification externe » une fois le débogage terminé pour éviter que des journaux supplémentaires ne soient écrits dans le fichier journal.

Note Une fois l'authentification externe activée, les utilisateurs peuvent la contourner pour un utilisateur spécifique, comme indiqué dans l'option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale). Cette option peut également être activée en accédant au flux de modification de l'utilisateur à partir du lien grâce au message d'avertissement lorsque l'authentification externe est également activée.

L'authentification externe à l'aide de SSO est l'approche d'authentification recommandée si la Fédération est activée.

Note À partir de la version 3.7. et ultérieures, la durée d'éviction d'une session d'authentification externe passe de six à neuf heures. Ce paramètre est applicable pour l'authentification externe ou sur site uniquement.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent configurer l'authentification externe. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **External Authentication (Authentification externe)**.

Figure 547: Configuration de l'authentification externe

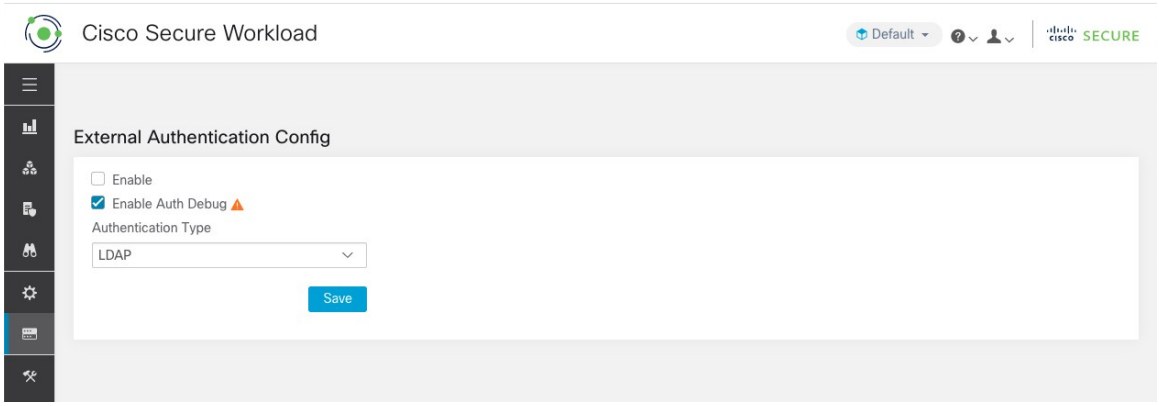


Figure 548: Configuration de l'authentification externe (Suite)

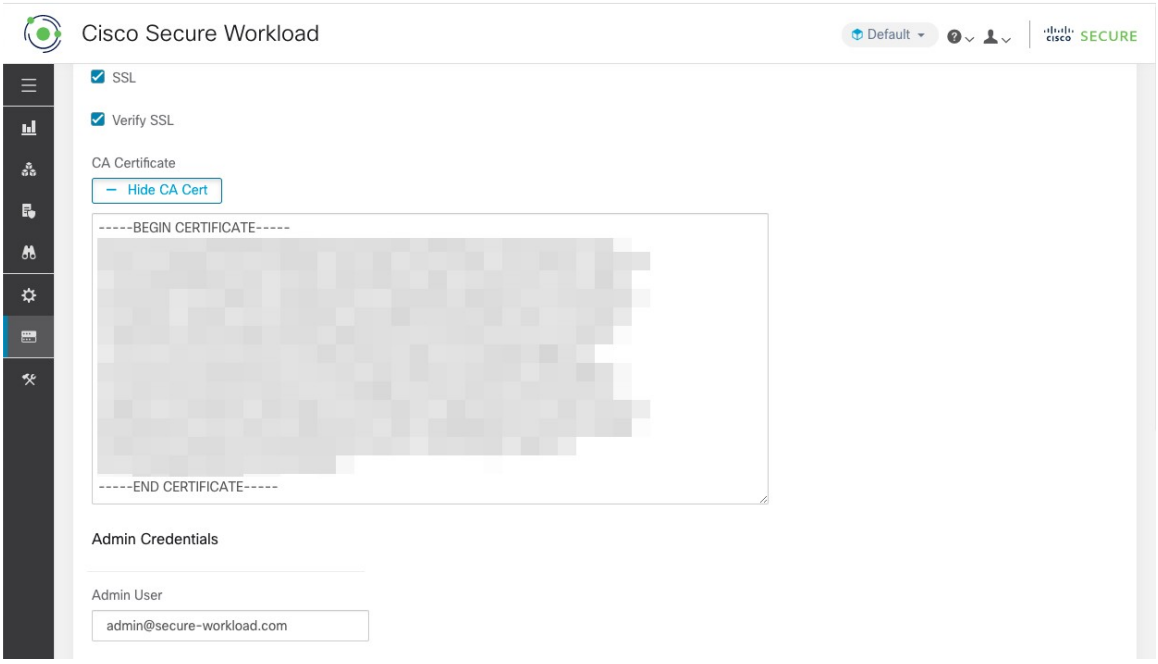


Figure 549: Configuration de l'authentification externe (Suite)

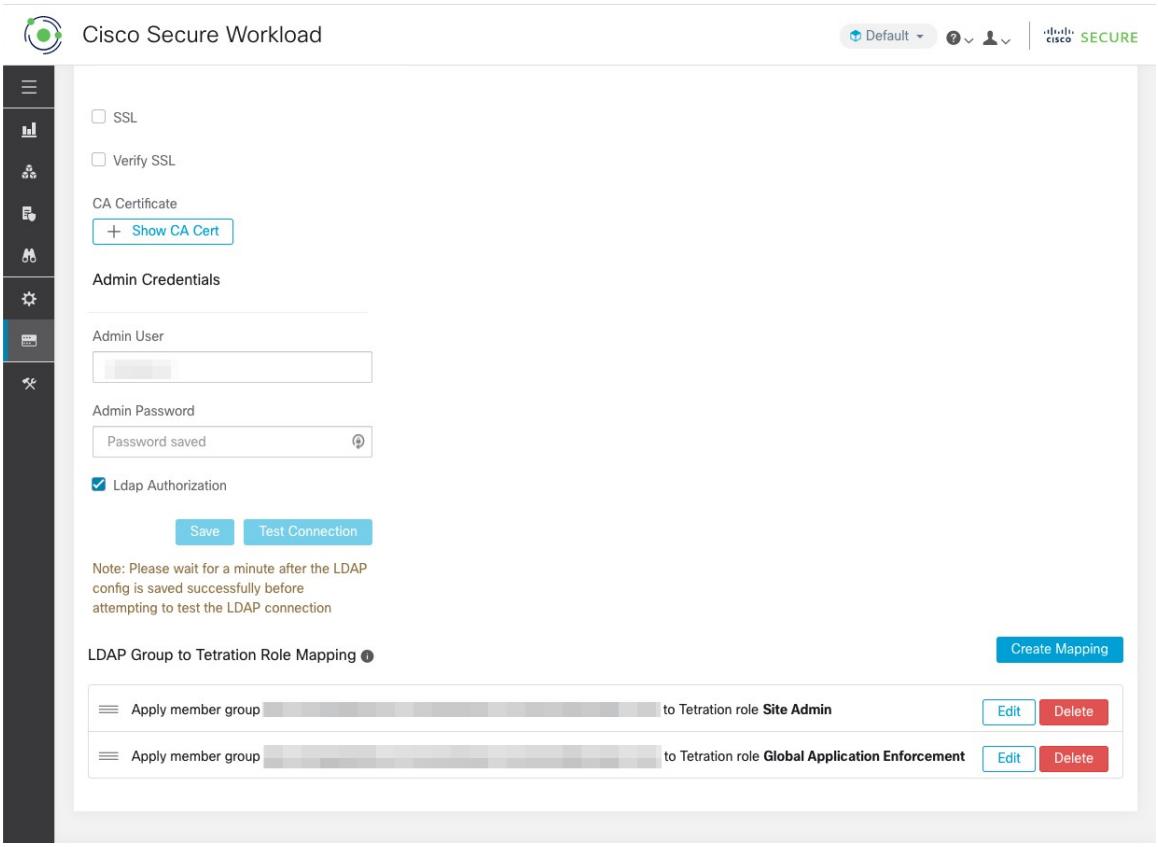
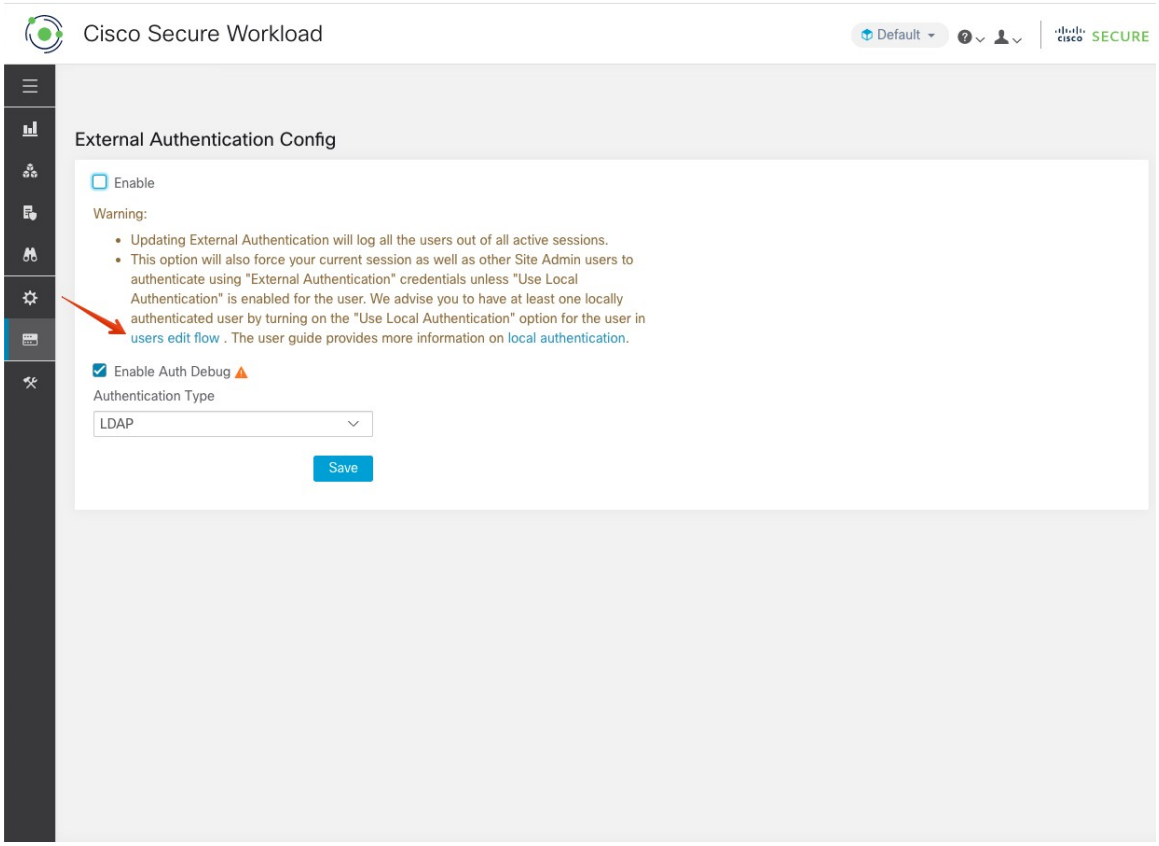


Figure 550: Avertissement relatif à l'authentification externe



Configuration du protocole LDAP (Lightweight Directory Access Protocol)

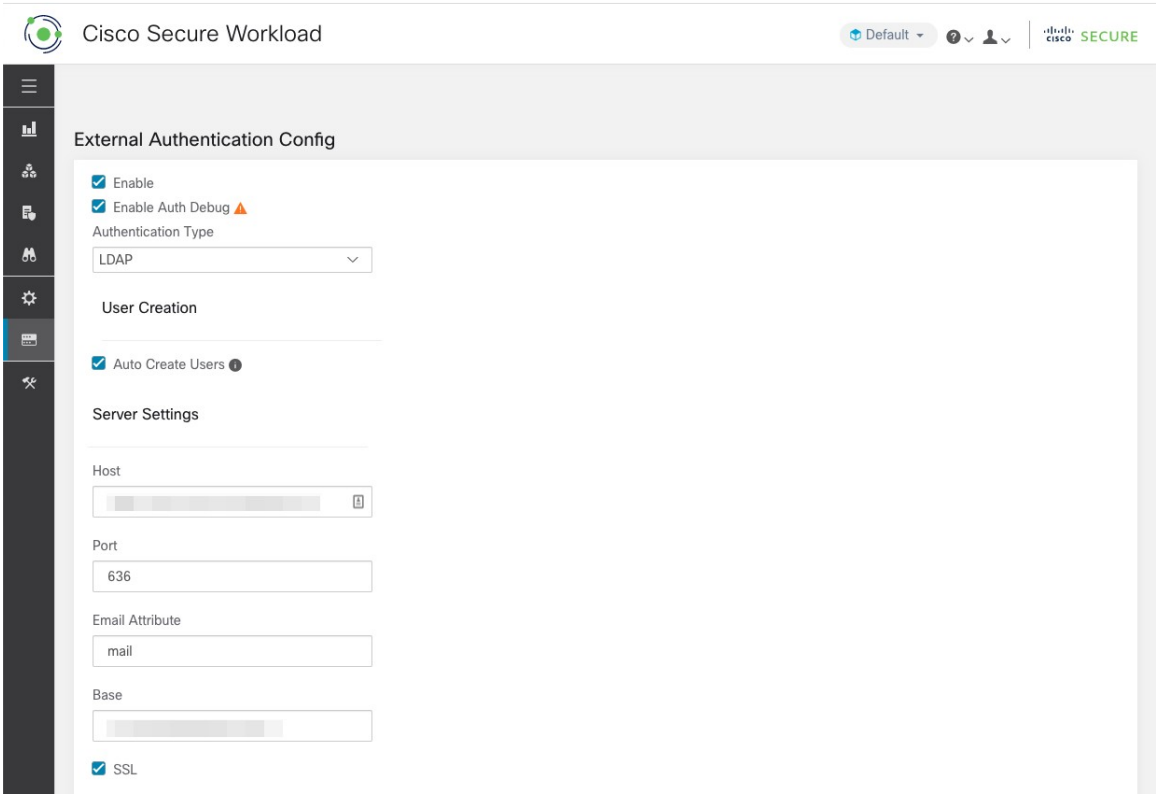
Choisissez l'option LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs. Cela signifie qu'une fois activée, tous les utilisateurs seront déconnectés et que les connexions ultérieures utiliseront leur adresse courriel et leur mot de passe LDAP pour s'authentifier.

LDAP n'est actuellement pas recommandé comme mécanisme d'authentification si la « Fédération » est activée.

Si LDAP est activé, le flux de travail recommandé pour la création de nouveaux utilisateurs est le suivant.

Les **administrateurs de site** sont invités à créer d'abord de nouveaux utilisateurs avec leurs courriels et à attribuer les rôles appropriés en Configurer l'autorisation LDAP (autorisation AD) avant que les nouveaux utilisateurs ne se connectent pour la première fois au moyen de LDAP. Si un nouvel utilisateur se connecte via LDAP sans jouer le rôle approprié, aucun rôle par défaut n'est attribué à l'utilisateur.

Figure 551: Configuration du protocole LDAP (Lightweight Directory Access Protocol)



Champ	Description
Créer des utilisateurs automatiquement	Si vous activez la création automatique des utilisateurs, des utilisateurs seront créés s'ils n'existent pas lors de la première connexion. Cela évite aux administrateurs du site d'avoir à mettre à disposition les utilisateurs avant de leur permettre de se connecter. Cette option doit être désactivée si l'accès Cisco Secure Workload est limité aux utilisateurs créés manuellement dans la page Utilisateurs.
Hébergement	Hôte LDAP qui sera utilisé pour l'authentification
Port	Port LDAP qui sera utilisé pour l'authentification.
Attribut du courriel	Nom d'attribut LDAP qui représente le courriel de l'organisation.
Base	Nom de domaine de base LDAP à partir duquel les utilisateurs seront recherchés.
SSL	Activez le chiffrement et utilisez « ldaps:// ».
Vérification SSL	Vérifier les attributs SSL du serveur tels que le nom de domaine complet (FQDN) en fonction du certificat du serveur.
Autorité de certification SSL Cert	Certificat de signature pour le certificat SSL du serveur LDAP Obligatoire si la chaîne de certificats du serveur ne peut pas être vérifiée publiquement.

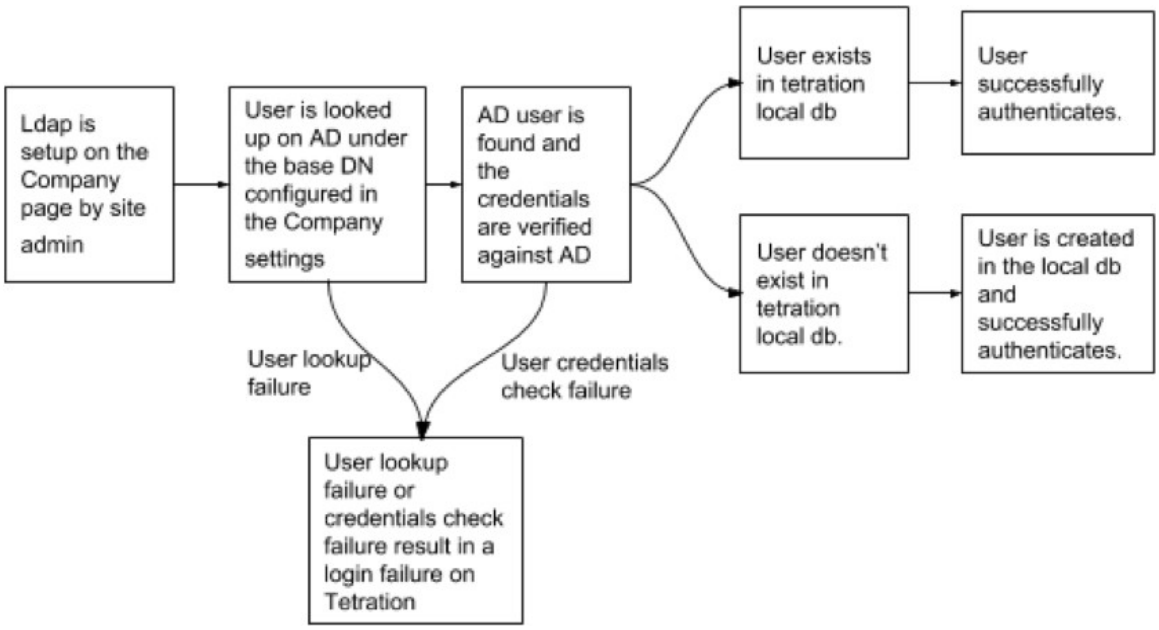
Champ	Description
Utilisateurs admin	Nom d'utilisateur admin LDAP (et non d'utilisateur Cisco Secure Workload) utilisé pour la liaison avec le serveur LDAP. Par exemple : [Utilisateur]@[Domaine] ou [Domaine]\\[Utilisateur]
Mot de passe de l'administrateur	Mot de passe d'administrateur LDAP utilisé pour la liaison avec le serveur LDAP.
Autorisation LDAP	L'autorisation LDAP peut être activée et configurée, comme expliqué dans Configurer l'autorisation LDAP (autorisation AD)

Une fois la configuration LDAP activée, tous les utilisateurs, à l'exception des utilisateurs avec l'option Option « Use Local Authentication » (Utiliser l'authentification locale) activée, seront déconnectés de leurs sessions.

La configuration LDAP peut être enregistrée après avoir cliqué sur le bouton **« Save »** (Enregistrer). Nous vous recommandons d'attenter une minute après l'enregistrement de la configuration LDAP avant de tenter de tester la connexion LDAP.

La connexion LDAP peut être testée après l'enregistrement de la configuration LDAP à l'aide du bouton **« Test Connection (Tester la connexion) »**. Cela tente une liaison avec le serveur LDAP avec les informations d'authentification d'administrateur saisies.

Figure 552: Flux de travail de l'authentification



Résoudre les problèmes LDAP

Si une erreur se produit lorsque vous testez la connexion LDAP, vérifiez les éléments suivants :

- Vérifiez si les informations d'authentification de l'administrateur LDAP sont correctes.
- Vérifiez les paramètres de connexion tels que l'hôte, le port, SSL, etc.
- Vérifiez si le serveur LDAP est accessible à partir des VIP de l'interface utilisateur Cisco Secure Workload.

- Vérifiez si le serveur AD est opérationnel.
- Utilisez les outils de ligne de commande tels que **« ldapsearch »** avec les renseignements de connexion pour vérifier si une liaison peut être établie.

Si une erreur se produit lors de la connexion d'un utilisateur, vérifiez les éléments suivants :

- Vérifiez si l'utilisateur peut se connecter avec ses renseignements d'authentification LDAP à d'autres sites Web de l'entreprise qui utilisent l'authentification LDAP.
- Vérifiez si le DN de base spécifié dans les paramètres LDAP de l'entreprise est correct. Cela peut être fait en utilisant des outils de ligne de commande tels que **« ldapsearch »** pour rechercher l'utilisateur dans le DN de base.

Exemple de requête **« ldapsearch »** pour rechercher un utilisateur par son adresse courriel :

```
ldapsearch -H "ldap://<host>:<port>" -b "<base-dn>" -D "<ldap-admin-user>" -w
<ldap->admin-password> "(mail=<users-email-address>)"
```

Configurer l'autorisation LDAP (autorisation AD)

L'autorisation Active Directory peut être configurée en cochant la case « LDAP Authorization » (Autorisation LDAP) dans la section « Admin Credentials » (Renseignements d'authentification d'administrateur) de la configuration LDAP d'authentification externe. Une fois ce paramètre activé, l'administrateur du site doit configurer les mappages des groupes « MemberOf » (Membre de) LDAP avec les rôles Cisco Secure Workload dans la section ci-dessous. Par défaut, sans cette configuration, les utilisateurs d'Active Directory doivent être préconfigurés avec un ou plusieurs rôles Cisco Secure Workload avant une tentative de connexion.

Le mappage du groupe LDAP MemberOf vers Cisco Secure Workload doit être configuré si l'authentification externe LDAP est activée. L'option « Create Mapping » (créer un mappage) permet de configurer le mappage d'une valeur de groupe LDAP MemberOf à un rôle Cisco Secure Workload. Les rôles dans la liste déroulante des rôles sont préremplis en fonction de la portée sélectionnée dans le sélecteur de portée. Une fois que ces mappages sont enregistrés, tous les utilisateurs sont autorisés en fonction de ces valeurs lors de leur connexion ultérieure.

Ces mappages peuvent être réorganiser, modifiés ou supprimés. Toute modification des mappages sera reflétée dans les rôles attribués aux utilisateurs lors de leurs connexions ultérieures. Un maximum de 50 mises en correspondance de rôles LDAP MemberOf avec Cisco Secure Workload peut être créé.

Les noms de groupe MemberOf LDAP en double ne sont pas autorisés. Cependant, plusieurs groupes LDAP MemberOf peuvent être mappés au même rôle. Si plusieurs groupes sont mappés au même rôle, le dernier mappage sera stocké dans l'utilisateur en tant que MemberOf LDAP correspondant au rôle Cisco Secure Workload.

Figure 553: Configuration du groupe LDAP vers le rôle Cisco Secure Workload

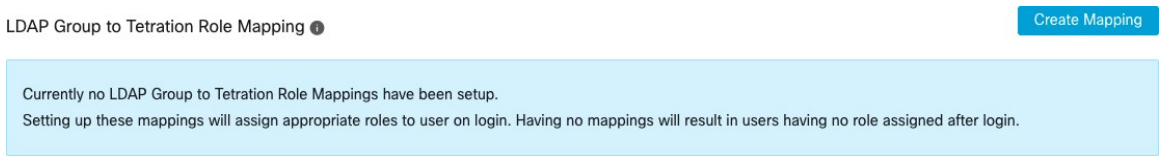
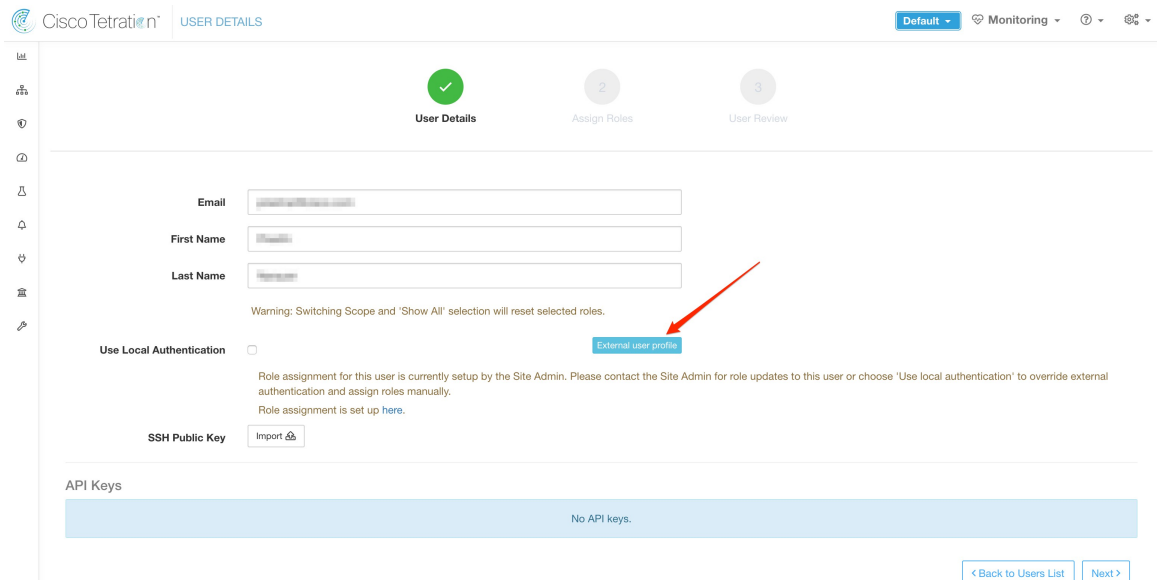


Figure 554: Mappage du groupe LDAP au rôle Cisco Secure Workload

Un utilisateur administrateur de site peut rapprocher l'attribution des rôles sur la base du mappage des rôles ci-dessus à l'aide des informations de l'utilisateur externe obtenues lors de la dernière connexion réussie de ce dernier.

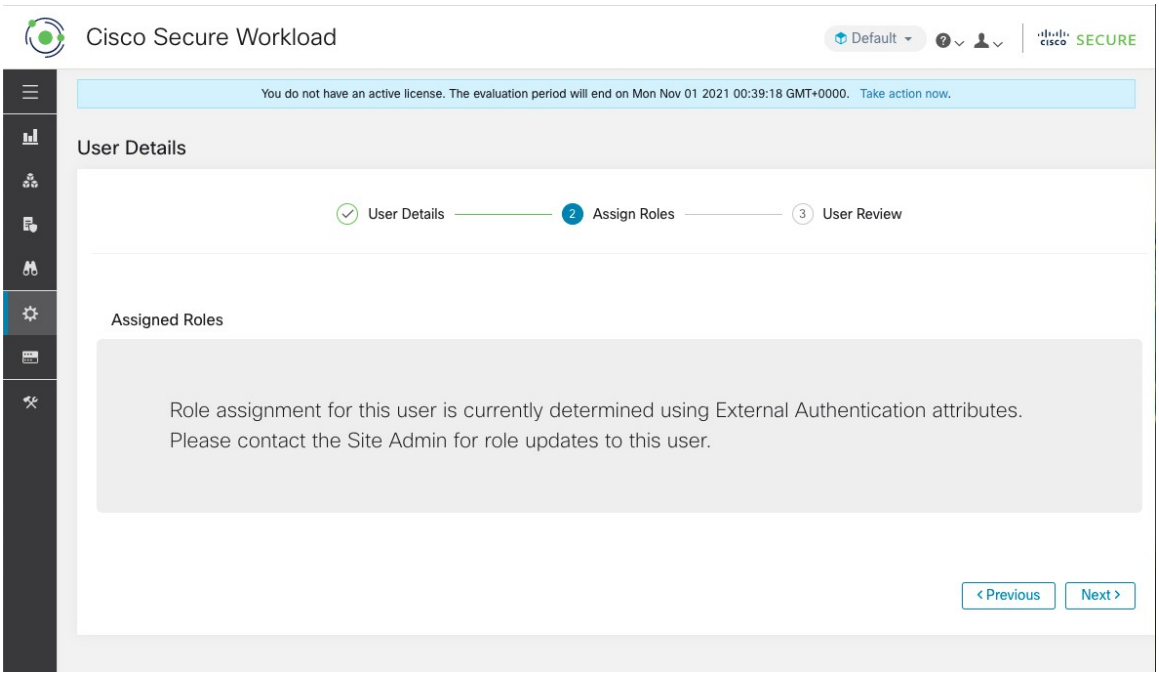
Note Une fois l'authentification externe activée, les utilisateurs peuvent la contourner pour un utilisateur spécifique, comme indiqué dans l'option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale). Ces utilisateurs contourneront également le processus d'autorisation configuré pour l'autorisation AD.

Figure 555: Renseignements sur l'utilisateur externe



Une fois l'autorisation activée, la sélection manuelle du rôle Cisco Secure Workload dans les flux de création d'utilisateurs (Ajouter un utilisateur, on page 928) et de modification d'utilisateurs (Modifier les détails ou le rôle d'un utilisateur) est **interdite**.

Figure 556: Page Utilisateurs



Les groupes MemberOf LDAP mappés aux rôles Cisco Secure Workload sont visibles sur la page de profil d'utilisateur.

Figure 557: Page Profil d'utilisateur

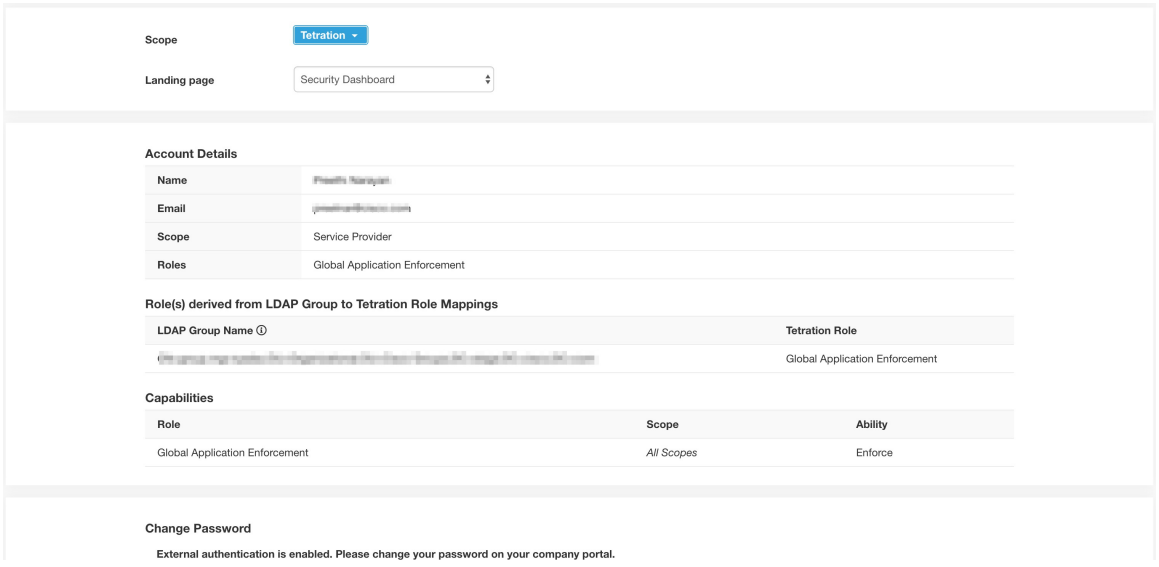
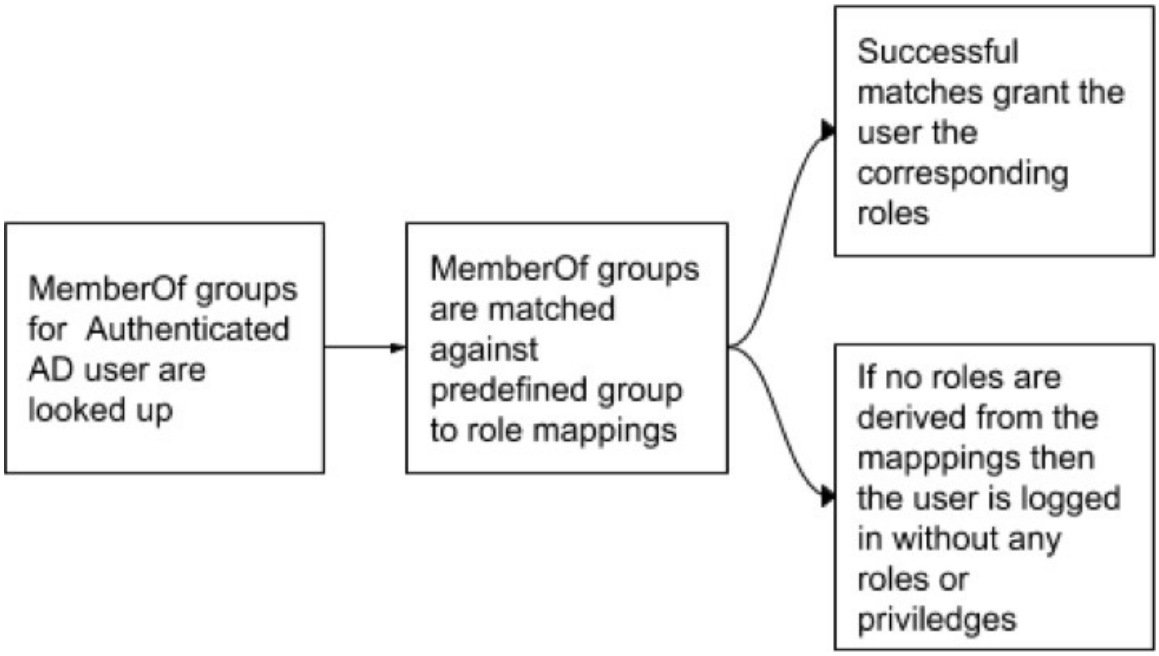


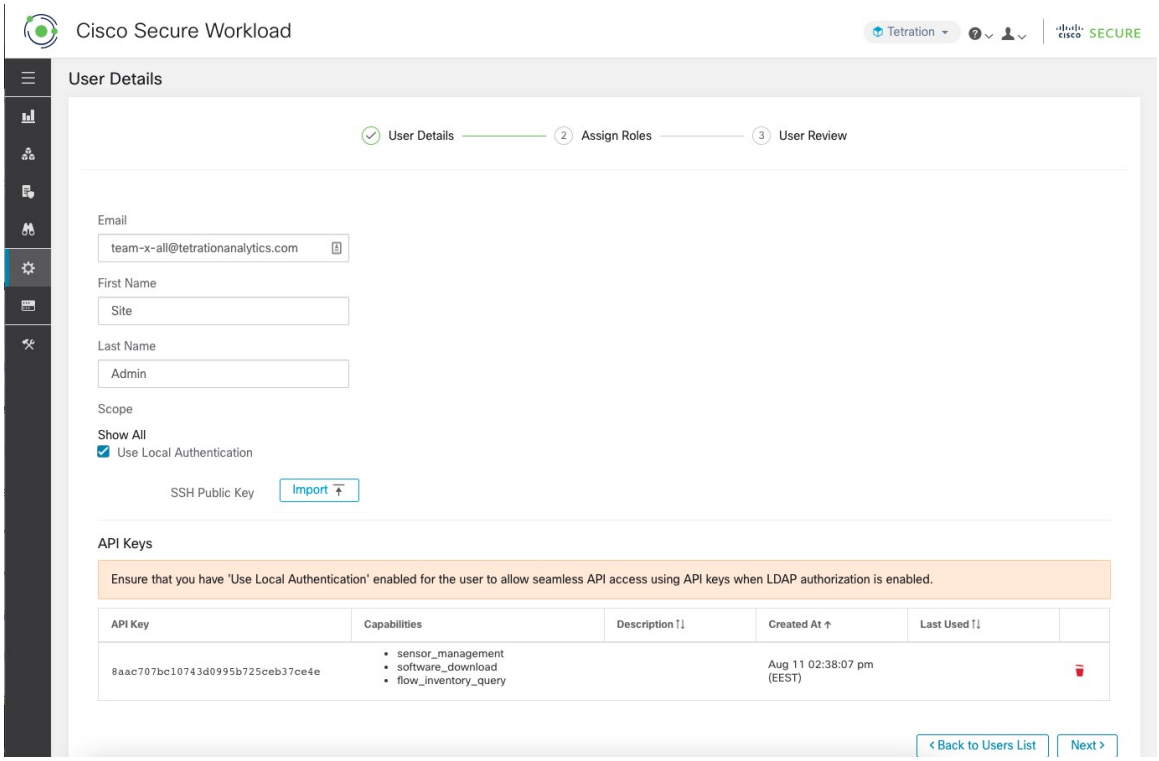
Figure 558: Flux de travail d'autorisation



Si l'autorisation LDAP est activée, l'accès à l'OpenAPI via les clés API ne fonctionne plus de manière transparente, car les rôles Cisco Secure Workload découlant des groupes LDAP MemberOf sont réévalués une fois la session de l'utilisateur terminée. Par conséquent, pour assurer un accès OpenAPI ininterrompu, nous recommandons aux utilisateurs dotés de clés API d'activer l'option Option « Use Local Authentication » (Utiliser l'authentification locale).

Figure 559: Avertissement lié à la clé API d'autorisation LDAP

Figure 560: Avertissement lié à la clé API d'autorisation LDAP sur la page Users (Utilisateurs)



Dépannage des problèmes d'autorisation LDAP

Si les rôles ne sont pas attribués aux utilisateurs en fonction des mappages définis dans la section « Mappages du groupe LDAP aux rôles », vérifiez de nouveau la configuration et le format des mappages de rôles.

- La chaîne de groupe doit être au format de chaîne . Par exemple : CN=group.jacpang,OU=Organizational,OU=Cisco Groups,DC=stage,DC=cisco,DC=com
- Les noms des groupes doivent être identiques à ceux qui figurent dans AD, sans espaces ni caractères supplémentaires.
- Le mappage de rôles pour le groupe doit être sélectionné à partir du sélecteur de rôles.

Étapes de débogage du mappage des rôles d'utilisateur

- Vous devez avoir deux utilisateurs, dont l'un est l'administrateur du site. Le courriel de cet utilisateur ne doit pas être la même que celui de l'utilisateur AD.
- Cet utilisateur est appelé « utilisateur SA » pour les étapes ci-dessous.
  - L'utilisateur SA a déjà configuré les configurations de mappage de rôles sur la configuration d'authentification externe de la page de l'entreprise, comme décrit précédemment. Supposons qu'un « utilisateur SA » se connecte avec le courriel [site-admin]@[domaine].
  - Nous supposons que l'« utilisateur AD » est [ad-admin] @ [domaine]. Nous supposons que la configuration LDAP est terminée et que l'utilisateur AD est en mesure de se connecter, mais n'obtient pas le rôle qui lui est attribué.

- En tant qu'utilisateur AD, connectez-vous en utilisant une session de navigateur de navigation privée. Cela sépare l'état du navigateur de la session d'utilisateur SA.
- En tant qu'utilisateur SA, connectez-vous et accédez à la page Users (utilisateurs).
- Cliquez sur l'icône Edit (modifier) pour l'utilisateur AD pour lequel le mappage des rôles doit être configuré.
- Cliquez sur le bouton « External User Profile » (profil d'utilisateur externe) sur la page User Profile (Profil de l'utilisateur).
- Vous verrez un tableau de profils d'authentification externe qui comprend une section « memberof » (membre de).
- Il s'agit de l'une des valeurs « memberof » que vous pouvez utiliser pour le mappage des rôles sur la page de l'entreprise, la configuration d'authentification externe, du groupe LDAP à la section de mappage des rôles.
- Vous devez fournir la chaîne par ligne complète « memberof » pour établir la correspondance. Une fois que vous avez créé ce mappage de rôles, toute personne ayant le même attribut « memberof » se verra attribuer le rôle mappé.
- Pour que l'utilisateur AD reçoive le nouveau rôle mappé, l'utilisateur doit se déconnecter, puis se reconnecter pour permettre la réévaluation de ce profil de mappage.
- Une fois qu'un utilisateur se connecte et que des rôles sont attribués avec succès à la suite des mappages de rôles de groupe, les règles de correspondance sont visibles sur la page « Preferences » (Preferences) de cet utilisateur.

Configurer la connexion unique (SSO)

Si cette option est sélectionnée, la connexion unique (SSO) peut être utilisée pour authentifier les utilisateurs. Cela signifie que lorsque cette option est activée, tous les utilisateurs sont redirigés vers la page de connexion du fournisseur d'identité pour s'authentifier. Les utilisateurs dont l'option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale) est activée peuvent utiliser le courriel et le mot de passe de connexion de la page de connexion pour s'authentifier.

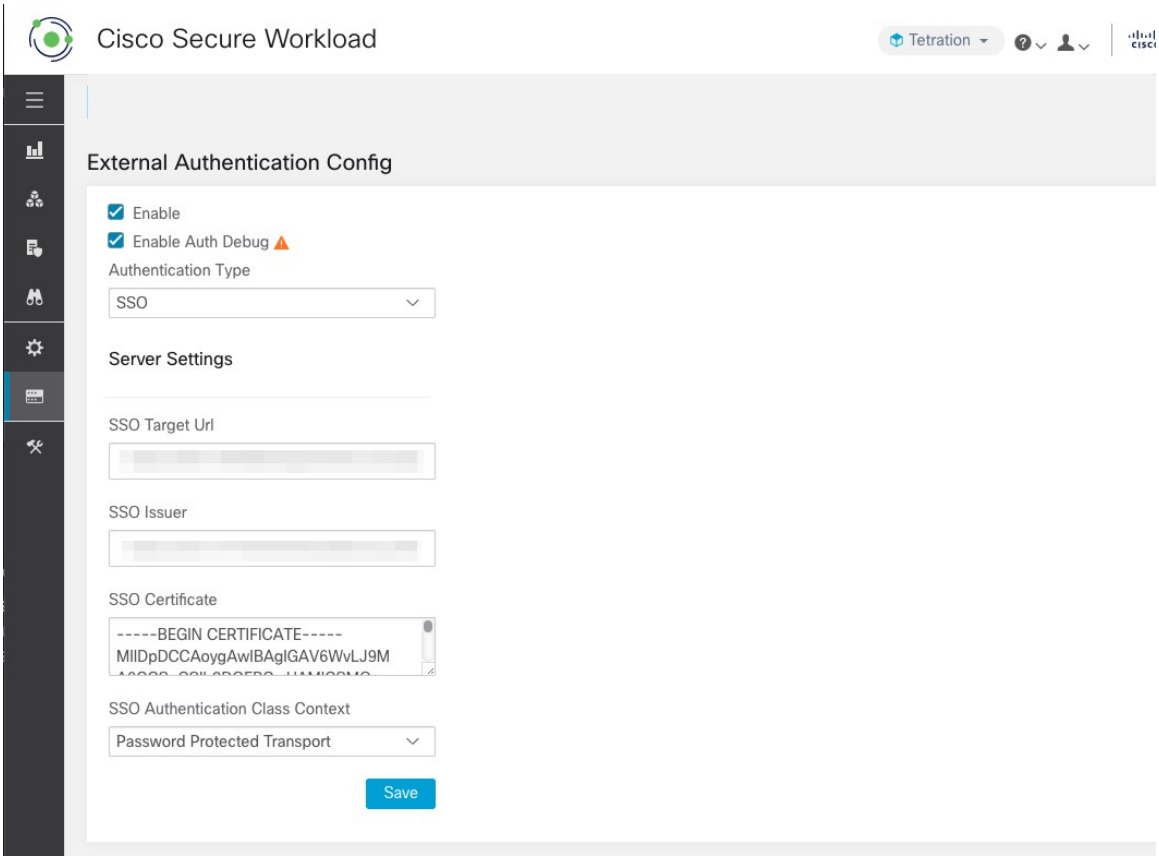
Il est important d'établir que la configuration SSO est configurée correctement, en particulier si aucun utilisateur n'utilise l'option Option « Use Local Authentication » (Utiliser l'authentification locale). L'approche recommandée est d'avoir au moins un utilisateur authentifié localement avec des informations d'authentification d' **Site Admin** (administrateur de site) en activant l'option Option « Use Local Authentication » (Utiliser l'authentification locale) (Utiliser l'authentification locale). Cet utilisateur peut s'assurer que la configuration SSO est mise en place correctement. Une fois la connexion configurée avec succès, cet utilisateur peut également être transféré vers l'authentification externe en décochant l'option « Use Local Authentication » dans le flux de modification de l'utilisateur.

Si SSO est activée, le flux de travail recommandé pour la création de nouveaux utilisateurs est le suivant.

Les **administrateurs du site** et les **propriétaires de portée** sont invités à créer d'abord de nouveaux utilisateurs avec leurs adresses de courriel et à attribuer les rôles et les portées appropriés avant que le nouvel utilisateur ne se connecte pour la première fois via SSO. Si un nouvel utilisateur se connecte via SSO sans jouer le rôle approprié, aucun rôle par défaut n'est attribué à l'utilisateur.

Le tableau suivant décrit les champs qui doivent être définis pour configurer SSO sur Cisco Secure Workload. Cisco Secure Workload est le fournisseur de services (FS) dans ce cas.

Figure 561: Configuration de la connexion unique

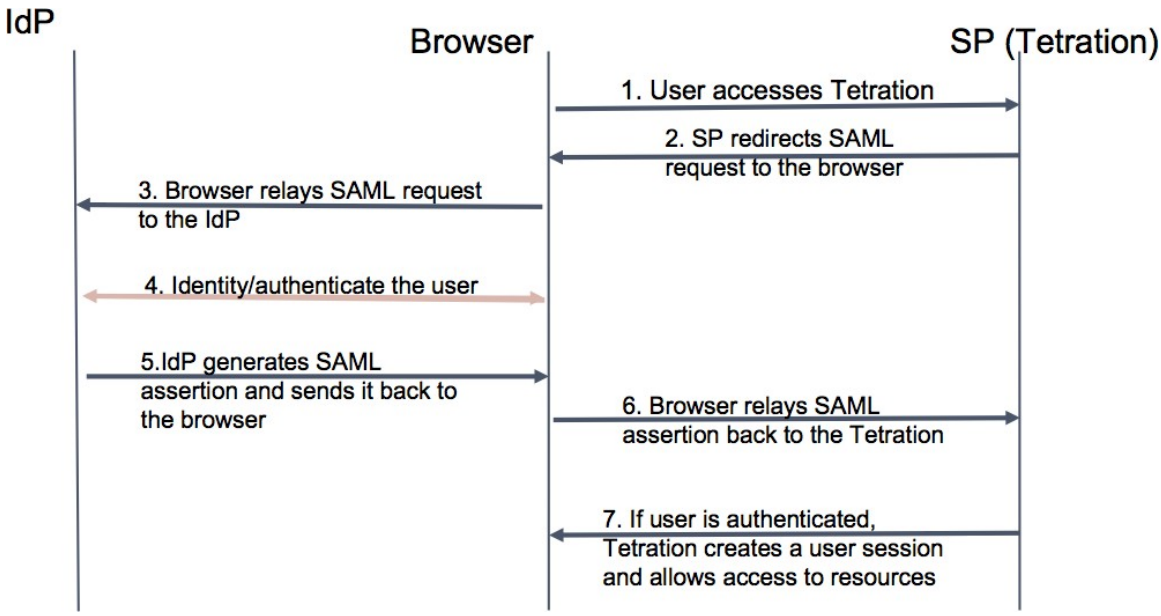


Champ	Description
URL SSO cible	URL cible du fournisseur d'identité SSO vers laquelle les utilisateurs seront redirigés pour la connexion.
Émetteur SSO	ID d'entité SSO de votre fournisseur de services, une URL qui identifie de manière unique votre fournisseur de services. Il s'agit généralement des métadonnées du fournisseur de services. Dans ce cas, il s'agit de : `https://<tetration-cluster-fqdn>/h4_users/saml/metadata`
Certificat SSO	Certificat SSO fourni par le fournisseur d'identité (IdP).
Contexte d'authentification SSO	Choix du contexte AuthN SSO spécifié dans la demande SAML. L'option par défaut est « Password Protected Transport » (transport protégé par un mot de passe). Les autres options sont « Authentification Windows intégrée » et « Certificat X.509 » pour l'authentification basée sur Windows et PIV.

Une fois la configuration SSO activée, tous les utilisateurs, à l'exception de ceux qui ont activé l'option Use Local Authentication, sont déconnectés de leurs sessions.

La configuration SSO est enregistrée lorsque vous avez cliqué sur le bouton **Save** (enregistrer).

Figure 562: Flux de travail de l'authentification



Renseignements partagés avec le fournisseur d'identité (IdP)

Le fournisseur d'identité a besoin de certaines informations de Cisco Secure Workload (SP) pour configurer le SSO en vue de l'authentification. Le tableau suivant décrit les champs qui doivent être configurés.

Champ	Description
URL SSO	Le point terminal d'authentification (URL) qui utilisera l'assertion SAML (réponse de l'IdP). Dans notre cas, ce sera : `https://<tetration-cluster-fqdn>/h4_users/saml/auth`
Identifiant de l'entité	Il s'agit des métadonnées pour le fournisseur de services. Dans ce cas, il s'agit de : `https://<tetration-cluster-fqdn>/ h4_users/saml/metadata`
Format de l'ID du nom	NameId est un courriel, c'est-à-dire `'urn:oasis:names:tc:SAML:1. 1:nameid-format:emailAddress'`
Attributs	que les attributs d'utilisateur sont extraits de l'IdP. Nous récupérons ces attributs dans le cadre de l'authentification : • e-mail • Prénom • Nom Assurez-vous que les noms d'attributs sont tels que spécifiés précédemment.

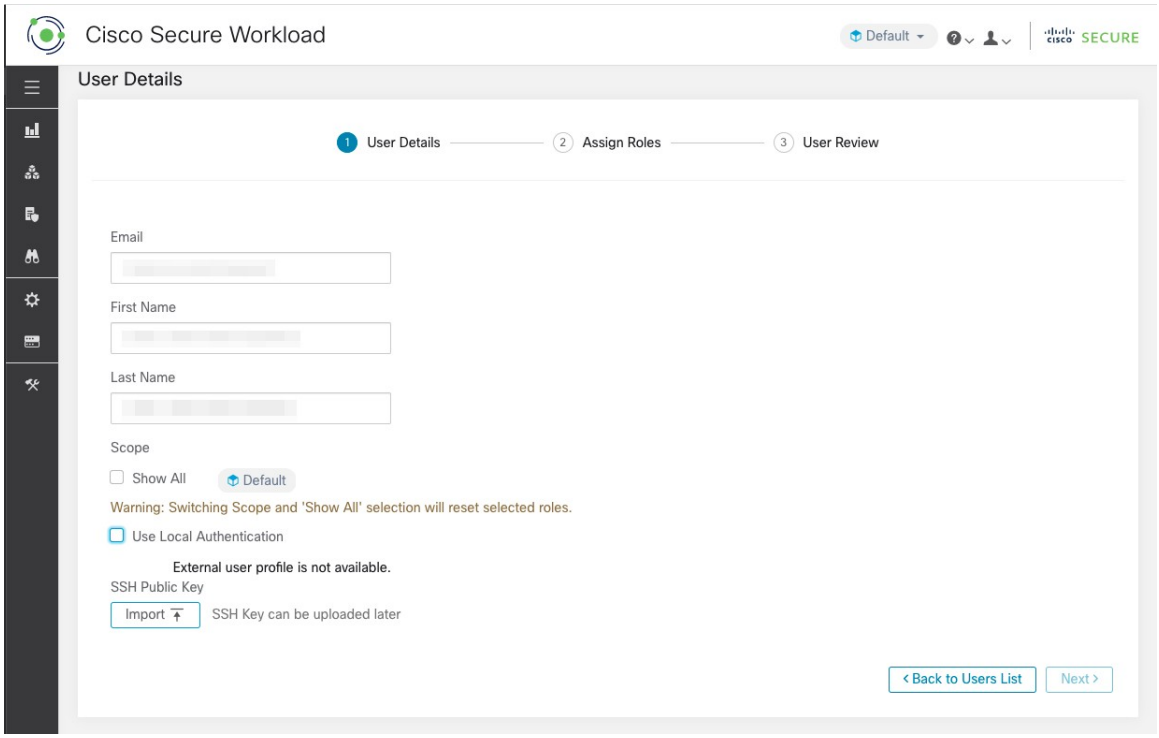
Résoudre les problèmes SSO

- Prévoyez un temps d'arrêt pour cette configuration SSO, car la seule façon de vérifier que l'authentification fonctionne (pour le fournisseur de services) est de l'avoir configurée.
- Vérifier et valider les métadonnées du fournisseur d'identité générées.
- Vérifier tous les paramètres de configuration qui sont échangés entre le fournisseur d'identité et le fournisseur de service.
  - Configuration au niveau du fournisseur d'identité : URL SSO, auditoire, ID de nom, attributs, etc.
  - Configuration sur la page de l'entreprise Cisco Secure Workload : URL de la cible SSO, émetteur SSO et certificat SSO.
- Obtenez un exemple d'assertion SAML renvoyée par le fournisseur d'identité à partir des journaux d'applications du serveur. Validez-le par rapport à un validateur SAML pour vous assurer qu'il s'agit d'une réponse SAML valide.
- Des erreurs dans la configuration du fournisseur de service SSO peuvent entraîner une erreur générée par le fournisseur d'identité. À l'aide de l'élément d'inspection du navigateur, vous pouvez voir les demandes réseau en cours.
- Si un utilisateur rencontre des problèmes pour se connecter, demandez à l'administrateur du fournisseur d'identité de vérifier si l'utilisateur a accès à l'application Cisco Secure Workload.

Option « Use Local Authentication » (Utiliser l'authentification locale)

Une fois la configuration mise en place, il est possible pour les administrateurs de site d'autoriser les utilisateurs à ne pas utiliser l'authentification externe. Cela peut être fait pour chaque utilisateur en activant l'indicateur « Use Local Authentication » (Utiliser l'authentification locale) dans la section de modification de l'utilisateur. La sélection de ce champ pour l'utilisateur déconnectera ce dernier de toutes les sessions.

Figure 563: Use Local Authentication (Utiliser l'authentification locale)



Warning **Assurez-vous qu'au moins un utilisateur dispose d'un accès à l'authentification locale!**

Si l'option « Use Local Authentication » est supprimée pour un utilisateur et que cet utilisateur est le dernier disposant de l'option, aucun utilisateur ne pourra se connecter à Cisco Secure Workload. Cela signifie qu'aucun utilisateur ne peut se connecter en cas de perturbations avec le système d'authentification externe, telles que des problèmes de configuration, de connectivité, etc. Vous verrez un avertissement si vous essayez de supprimer le dernier utilisateur authentifié localement.

Les utilisateurs se connectant par authentification externe ont des sessions plus courtes et seront invités à se connecter à l'expiration de la session. Les utilisateurs qui se connectent par authentification externe ne peuvent pas réinitialiser leur mot de passe sur le site (ils doivent le faire sur le site Web de leur entreprise). Toutefois, si l'indicateur « Use Local Authentication » est activé pour l'utilisateur, la réinitialisation du mot de passe est possible.

Certificat et clé SSL

Pour activer un accès HTTPS entièrement vérifiable à l'interface utilisateur Cisco Secure Workload, un certificat SSL spécifique au nom de domaine de l'interface utilisateur et à la clé privée RSA qui correspond à la clé publique du certificat SSL peut être téléversé dans la grappe.

Un certificat SSL peut être obtenu de deux manières, en fonction du format du nom de domaine complet (FQDN) utilisé pour faire référence à l'adresse IP virtuelle (VIP) de l'interface utilisateur Cisco Secure Workload. Si le nom de domaine complet Cisco Secure Workload est basé sur un nom de domaine d'entreprise comme tetration.cisco.com, l'autorité de certification (CA) de votre entreprise qui possède le domaine de base

vous délivre un certificat SSL. Sinon, vous pouvez utiliser un fournisseur de certificat SSL réputé pour vous délivrer un certificat SSL pour votre nom de domaine complet.

Note Il est important de noter que même si l'interface utilisateur Cisco Secure Workload prend en charge Server Name Indication (SNI), les autres noms de sujets (SAN) spécifiés dans le certificat ne seront pas mis en correspondance. Par exemple, si le nom commun (CN) du certificat est tetration.cisco.com et que le certificat inclut un SAN pour tetration1.cisco.com, les requêtes HTTPS envoyées avec un navigateur compatible SNI vers la grappe avec tetration1.cisco.com comme nom d'hôte ne seront pas servies avec ce certificat. Les demandes HTTPS faites à la grappe avec un nom d'hôte autre que le nom d'hôte spécifié dans le CN seront traitées à l'aide du certificat autosigné par défaut qui est installé sur la grappe. Ces demandes entraînent des avertissements du navigateur.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent utiliser des certificats SSL. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **SSL Certificate (Certificat SSL)** .

Pour importer le certificat et la clé, cliquez sur le bouton **Import New Certificate and Key** (Importer le nouveau certificat et la clé).

Note La première importation de la certification SSL et de la clé privée doit être effectuée par l'intermédiaire d'une connexion réseau de confiance vers la grappe afin que la clé privée ne puisse pas être interceptée par des tiers malveillants qui ont accès à la couche de transport.

Saisissez les informations suivantes pour votre certificat SSL et votre clé :

NAME peut être n'importe quel nom pour la paire de clés de certificat. Ce nom vous sera utile lorsque vous chercherez à savoir quel certificat SSL est installé.

Le champ**Certificat X509** accepte la chaîne de certificat SSL au format Privacy Enhanced Mail (PEM). Si votre certificat SSL nécessite un groupe d'autorités de certification intermédiaire, concaténez le groupe d'autorités de certification après votre certificat de sorte que le certificat SSL pour votre nom de domaine complet Cisco Secure Workload se trouve au début du fichier de certificat.

Il doit avoir le format suivant :

```
-----BEGIN CERTIFICATE-----

< Certificat pour Nom de domaine complet Cisco Secure Workload>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<Contenu de l'autorité de certification intermédiaire 1>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<Contenu de l'autorité de certification intermédiaire 2>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
```

```
<Contenu de l'autorité de certification racine>

-----END CERTIFICATE-----
```

Le champ**Clé privée RSA** doit indiquer la clé privée RSA de la clé publique signée dans le certificat précédent. Il doit avoir le format suivant :

```
-----DÉBUT DE LA CLÉ PRIVÉE RSA-----

< données de la clé privée >

----FIN DE LA CLÉ PRIVÉE RSA----
```

Note La clé privée RSA doit être non chiffrée. Une « 500 Internal Server Error » (erreur du serveur interne 500) est émise si la clé privée RSA est chiffrée.

Après l'importation, des étapes de vérification sont exécutées pour s'assurer que la clé publique signée dans le certificat et la clé privée sont bien une paire de clés RSA. Si la vérification réussit, nous affichons le condensé SHA-1 (signature SHA-1 et heure de création) du lot de certificats.

Rechargez le navigateur pour constater que votre connexion SSL à l'interface utilisateur Cisco Secure Workload utilise maintenant le certificat SSL nouvellement importé.

Configuration de grappe

Cette section affiche la configuration d'exécution de la grappe Cisco Secure Workload pour le réseau et les contacts administratifs du client. Les valeurs modifiables sont indiquées par une icône en forme de crayon.

Note a. Strong SSL Chiffres for Agent Connections (chiffrements SSL forts pour les connexions d'agents) : lorsque cette option est activée, les protocoles TLS-1.0 et TLS-1.1 et les chiffrements suivants ne seront pas acceptés par la grappe Cisco Secure Workload pendant les négociations SSL : DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Les connexions suivantes les respectent et utilisent des chiffrements forts pendant l'établissement de liaison TLS :

1. Toutes les connexions d'API et d'interface utilisateur à Cisco Secure Workload.
2. Toutes les connexions des agents de visibilité et d'application à Cisco Secure Workload.

Remarque : les anciennes bibliothèques SSL peuvent ne pas prendre en charge cette option.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à ce paramètre. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)**.

Une fois la configuration modifiée, il faut un certain temps avant que la nouvelle configuration soit appliquée à l'ensemble de la grappe, ce qui est indiqué par la mise en surbrillance de la configuration particulière.

External IPv6 Cluster Connectivity

Physical Cisco Cisco Secure Workload clusters can be configured to connect to both external IPv4 and IPv6 networks. IPv4 connectivity is required but IPv6 connectivity is optional. Once IPv6 connectivity has been configured it can not be disabled. Enabling IPv6 connectivity for external networking for the cluster can only be done during deploy or upgrade. Please see the Cisco Cisco Secure Workload Upgrade Guide for more information about enabling external IPv6 cluster connectivity during upgrade or the Cisco Cisco Secure Workload Hardware Deployment Guide for more information about enabling external IPv6 cluster connectivity during deployment.

Before you begin

To get agents to operate in dual stack mode (supporting both IPv4 and IPv6)

Prerequisite

- Cluster must have IPv6 enabled.
- Create A and AAAA records (for IPv4 and IPv6) in DNS for a FQDN and wait for the domain names to resolve.

Configure “Sensor VIP FQDN” for agents to operate in dual stack mode

Procedure

Étape 1 Choose **Platform** > **Cluster Configuration** from the navigation bar on the left.

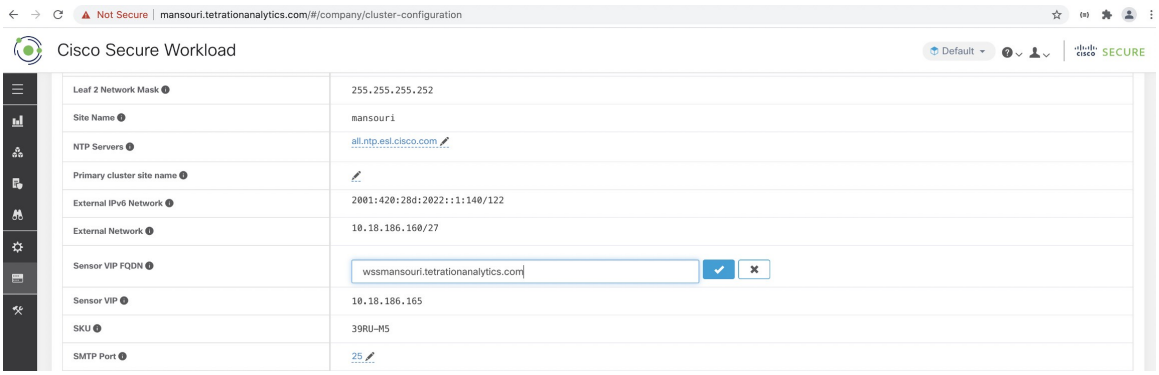
Étape 2 Look for the “Sensor IPv6 VIP”, “Sensor VIP” and “Sensor VIP FQDN” fields. “Sensor IPv6 VIP” and “Sensor VIP” should already be set.

Étape 3 If “Sensor VIP FQDN” is not set, set it to the FQDN created above. The A and AAAA records in DNS for the FQDN must resolve before you do this.

Étape 4 If “Sensor VIP FQDN” was already set, make sure there are A and AAAA records in DNS for the FQDN as set in the “Sensor VIP FQDN” field, then click into the “Sensor VIP FQDN” field and save it to the same value so it updates.

Étape 5 After the field completes updating (after about 20 minutes, the status is updated automatically), agents will be able to connect to the cluster via both IPv4 and IPv6.

Étape 6 Valid “Sensor VIP FQDN” can be set only once.



Note No IPv6 enforcement support for AIX. For more information on the requirements and limitations for dual-stack mode, see the Cisco Cisco Secure Workload Upgrade Guide

Authentification NTP

La version sur site de Cisco Secure Workload prend en charge la version 4 du protocole NTP (Network Time Protocol) et l'authentification SHA-1. Configurez le serveur NTP à l'aide de l'interface utilisateur de configuration ou utilisez la page de configuration de la grappe pour déployer l'appareil sur Cisco Secure Workload.

Pour configurer l'authentification NTP à l'aide de l'interface utilisateur de Cisco Secure Workload :

Procedure

Étape 1 Configurez le serveur NTP : Un système exécutant CentOS 7 fournit les configurations suivantes à titre de référence, et les configurations varient en fonction du système d'exploitation.

a) Assurez-vous que les entrées suivantes sont disponibles dans le dossier `/etc/ntp.conf`.

```
# Key file containing the keys and key identifiers used when operating with symmetric
key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
trustedkey 1
controlkey 1
requestkey 1
```

b) Saisissez la clé côté serveur sous `/etc/ntp/keys`.

```
# For more information about this file, see the man page ntp_auth(5).
# id type key
1 SHA1 <password>
```

c) Redémarrez le serveur NTP : `# service ntpd restart`

d) Démarrez le service pour le serveur NTP :

```
# ntpq -p
     remote           refid      st  t  when  poll  reach  delay  offset  jitter
==============================================================================
<ntp.server.com> <refid>      5  u  17     64     377  0.000  0.000   0.000
```

Étape 2 Sur l'interface utilisateur de Cisco Secure Workload, accédez à **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Dans le champ **Authenticated NTP Server** (serveur NTP authentifié), saisissez le nom ou l'adresse IP du serveur NTP.

Étape 4 Dans le champ **Password For Authenticated NTP Server** (mot de passe du serveur NTP authentifié), saisissez le mot de passe du serveur NTP.

Après avoir configuré et authentifié le serveur NTP, ce dernier prévaut sur tous les serveurs NTP non authentifiés que vous saisissez dans Cisco Secure Workload.

Désactiver le téléchargement et l'enregistrement des agents non pris en charge

En tant qu'administrateur système, vous avez la possibilité d'empêcher les agents dont les versions ne sont pas prises en charge de s'enregistrer auprès de la grappe ou d'être installés à l'aide du script d'installation. Cela est géré par une nouvelle configuration qui bloque efficacement les nouvelles installations d'agents dotés des versions obsolètes.

Par exemple, si vous utilisez Cisco Secure Workload version 3.9 et que l'agent que vous essayez de télécharger ou d'enregistrer utilise la version 3.7 ou une version antérieure, l'agent ne pourra pas télécharger ou s'enregistrer. Cette fonctionnalité est conçue pour garantir que tous les agents de la grappe fonctionnent sur des versions prises en charge, ce qui peut permettre de prévenir les problèmes de compatibilité ou les vulnérabilités de sécurité qui pourraient exister avec les anciennes versions du logiciel.

Désactiver les agents non pris en charge

Pour activer la configuration **Disable Unsupported Agents** (désactiver les agents non pris en charge), procédez comme suit :

Procedure

Étape 1 Connectez-vous à l'interface utilisateur de Cisco Secure Workload en tant qu'administrateur.

Étape 2 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Définissez le champ de configuration **Disable Unsupported Agents** (désactiver les agents non pris en charge) sur **True** (Vrai). Par défaut, cette fonction est désactivée.

What to do next

Après avoir activé la configuration, les agents dont les versions ne sont pas prises en charge ne pourront pas s'inscrire auprès de la grappe ou être installés à l'aide du script d'installation. Cela bloque efficacement l'installation des agents avec des versions obsolètes, garantissant que seules les versions d'agent prises en charge sont utilisées dans l'environnement.

Pour poursuivre l'inscription de l'agent, nous vous recommandons de télécharger la dernière version de l'agent logiciel.

Désactiver le téléchargement de l'agent

Pour empêcher l'installation d'agents ayant des versions de logiciels obsolètes, procédez comme suit :

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 2 Activez la configuration de **Disable Agent Download** (désactivation du téléchargement de l'agent).

Une fois la configuration activée, l'agent ne peut plus télécharger avec succès, quelle que soit la version de l'agent logiciel.

Désactiver l'enregistrement de l'agent

Pour empêcher l'enregistrement de nouveaux agents :

Procedure

Étape 1 Connectez-vous à l'interface utilisateur de Cisco Secure Workload en tant qu'administrateur.

Étape 2 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Activez la configuration de **Désactiver l'enregistrement de l'agent**. Après avoir activé la configuration, vous ne pouvez pas enregistrer de nouvel agent sur l'appareil qui ne correspond pas à la version du logiciel.

Note Après avoir activé la configuration, si vous tentez de télécharger ou d'enregistrer un agent avec une version non prise en charge, l'enregistrement sur l'appareil échoue et un message d'avertissement s'affiche sur l'interface graphique (GUI) indiquant : "Package download or registration for the old agent version is disabled." ("Le téléchargement ou l'enregistrement de paquets pour l'ancienne version de l'agent est désactivé.") Cela garantit que seuls les agents dont les versions sont prises en charge peuvent être enregistrés ou installés, ce qui empêche l'utilisation de versions d'agent obsolètes dans l'environnement.

Note Par défaut, les configurations **Disable Unsupported Agents (Désactiver les agents non pris en charge)**, **Disable Agent Download (Désactiver le téléchargement de l'agent)** et **Disable Agent Registration (Désactiver l'enregistrement des agents)** sont désactivées.

Analyse de l'utilisation

Les administrateurs de site et **les utilisateurs du service d'assistance à la clientèle** peuvent activer ou désactiver l'analyse de l'utilisation. Dans la barre de navigation, cliquez sur **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Usage Analytics (Analyse de l'utilisation)**.

Cisco Secure Workload collecte les données et les restitue de manière anonyme grâce au condensé unidirectionnel avant de les envoyer au serveur. Configurez les paramètres de confidentialité par appareil pour un appareil sur site et par détenteur pour le logiciel-service Cisco Cisco Secure Workload. Vous pouvez également activer la collecte de données et basculer la collecte sur cette page.

Federation

Federation provides a means of joining multiple Cisco Secure Workload appliances together and consolidating much of their management to a single appliance designated as the **leader**.

Note

- This feature requires all appliances in the federation to be running release 3.4.x or later.
- Contact Cisco Technical Assistance Center to enable the federation option.

Configurer la Fédération

Procédure

Étape 1 Sur le **leader** chef de file) désigné , accédez à **Platform(Plateforme)** > **Federation (Fédération)** et cliquez sur le bouton **Create New Federation** (Créer une nouvelle Fédération).

Étape 2 Pour ajouter le premier appareil **suiveur**, entrez son nom et son nom de domaine complet (FQDN), puis cliquez sur le bouton **Add** (ajouter).

Étape 3 Cliquez sur le lien pour télécharger le fichier de certificat de jonction.

Étape 4 Sur le **suiveur**, accédez à **Platform** > **Federation**, cliquez sur **Join Existing Fédération** (Rejoindre la Fédération existante), puis sélectionnez le certificat de jonction créé ci-dessus.

Étape 5 Répétez les étapes 2 à 4 pour chaque **suiveur** qui fera partie de la Fédération.

Illustration 564 : Créer ou rejoindre une Fédération

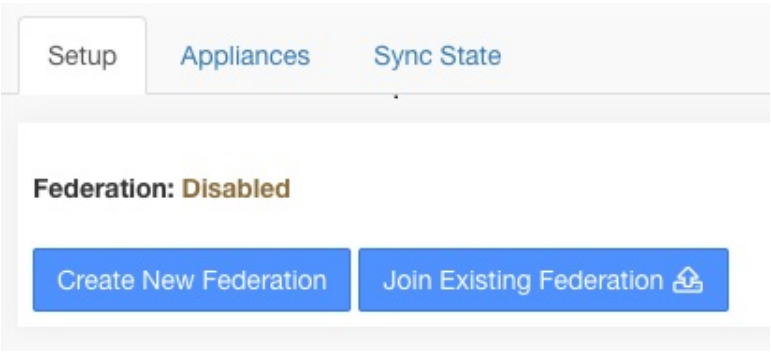
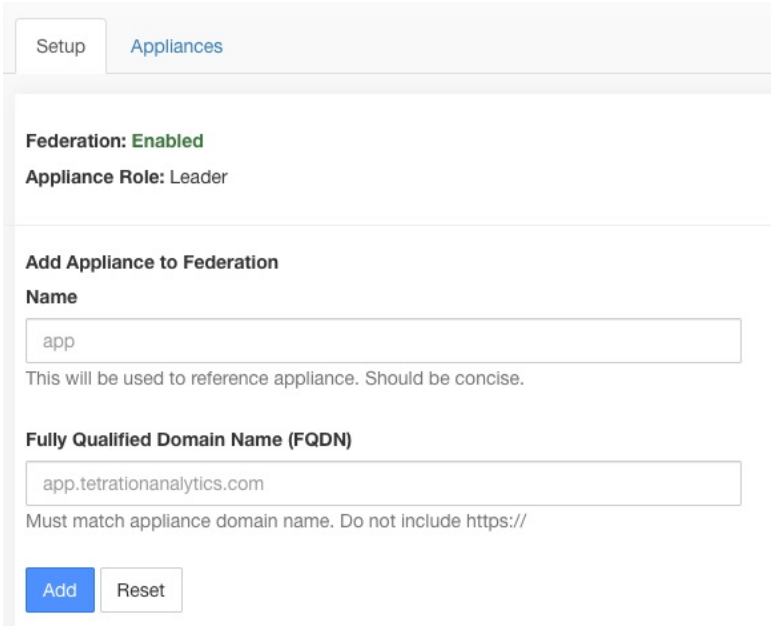
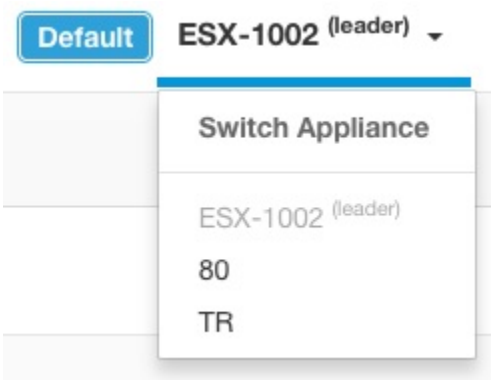


Illustration 565 : Formulaire d'ajout de suiveur à la Fédération



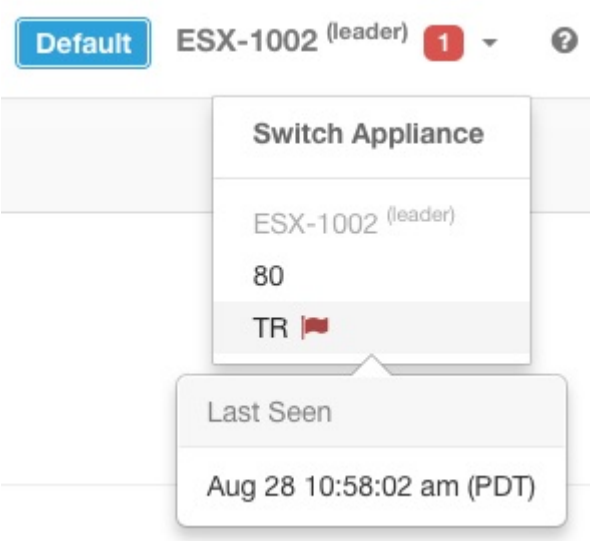
Lorsque la Fédération est activée, l'en-tête comprend le nom de l'appareil et un sélecteur pour la modification des appareils.

Illustration 566 : Sélecteur d'appareils



Si au moins un appareil de la Fédération n'a pas été vu par le chef de file après plus de 10 minutes, une alerte s'affiche dans le sélecteur d'appareils et les appareils problématiques sont signalés. Passer le curseur sur eux permet d'afficher la dernière fois qu'ils se sont synchronisés avec le chef de file.

Illustration 567 : Sélecteur d'appareils avec alertes



Configuration de l'authentification

L'authentification avec Fédération activée est configurée à l'aide de la connexion unique (SSO). La SSO doit être configurée sur chaque appareil de la Fédération. La configuration de la SSO est configurée sur le leader (chef de file) et chacun des suiveurs sur la page d'**authentification externe** > **de la plateforme** , comme indiqué dans la section Configurer la connexion unique (SSO) sur chaque appareil.

Tâches administratives

Selon la tâche administrative, certaines doivent être effectuées sur le **leader (chef de file)** et d'autres sur les **suiveurs**. Le tableau suivant indique le type d'appareil pour chaque tâche.

Tableau 49 : Tâches administratives dans l'appareil de Fédération

Tâche	Appareil
Utilisateurs	Chef de file
Portées	Chef de file
Rôles	Chef de file
Détenteurs	Chef de file
Clé API	Chef de file
Règles de collecte	Chef de file
Configuration de l'agent logiciel	Chef de file
Agents logiciels	Suiveurs

Tâche	Appareil
Mise à niveau de l'agent logiciel	Suiveurs
Rétrogradation de l’agent logiciel	Suiveurs
Filtres d’inventaire	Chef de file
Téléversement de l’inventaire	Chef de file
Configuration par défaut de la découverte des politiques	Chef de file
Ordre des politiques	Chef de file

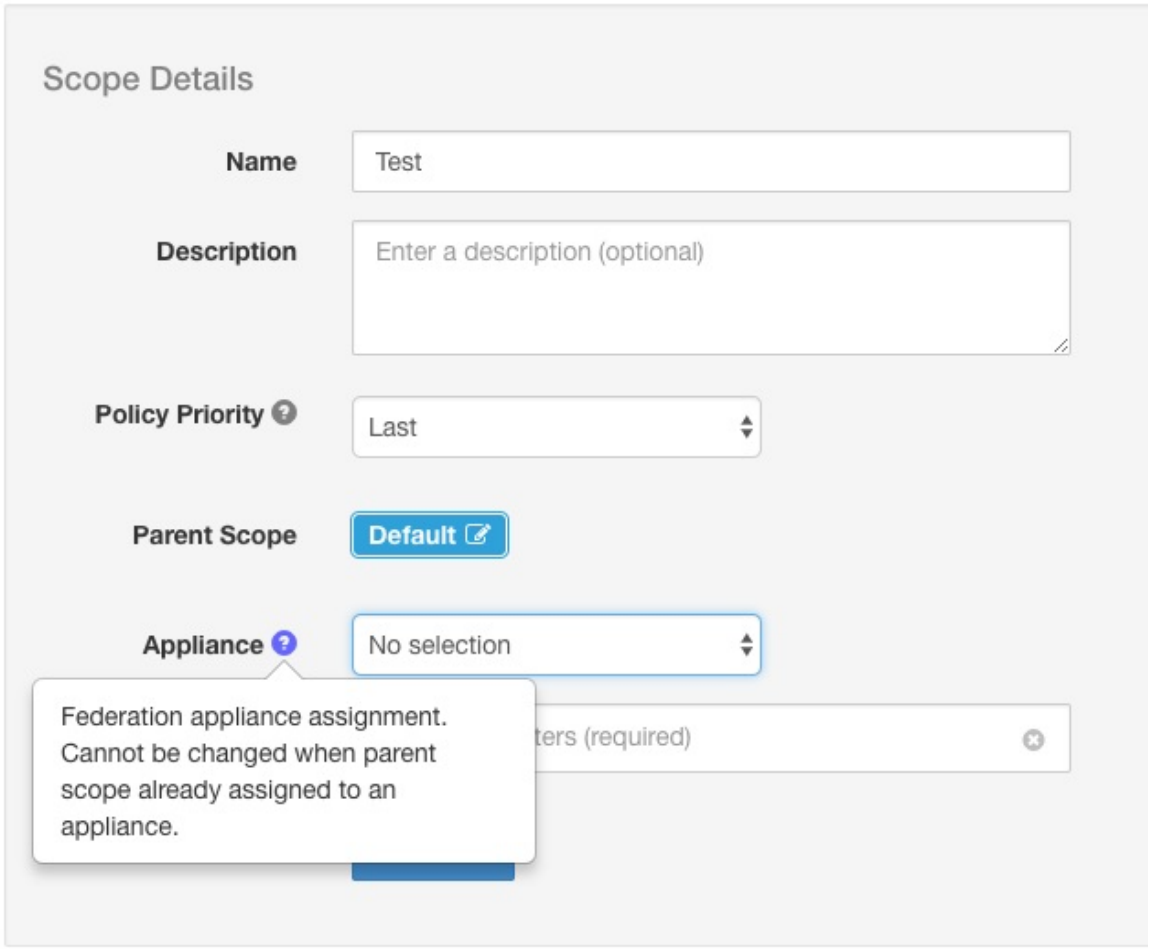
Portées

Lorsque l'inventaire d’une portée est géré par un seul appareil, cette portée peut être attribuée à l’appareil. Cela permet la découverte, l’analyse et l’application automatiques des politiques dans les espaces de travail associés à cette portée. Cela garantit également que les politiques créées sur cette portée s’appliquent uniquement aux agents connectés à l’appareil.

Les applications créées sur des portées globales (non affectées à un appareil) ne peuvent pas être utilisées pour la découverte ou l’analyse automatique des politiques. Cependant, elles peuvent être utilisées pour appliquer les politiques sur tous les appareils de la Fédération.

Un appareil peut être affecté à une portée lors de la création ou en modifiant la portée. Toutes les portées enfants héritent de l’appareil parent et ne peuvent pas être affectées à un autre appareil.

Illustration 568 : Affecter l'appareil à la portée



Remarque Les portées au niveau racine (détenteurs) sont toujours globales et ne peuvent pas être affectées à un appareil.

Espaces de travail

Tous les espaces de travail (« applications ») doivent être gérés sur l'appareil **chef de file**. Cependant, les organigrammes basés sur les flux ne peuvent être affichés que sur l'appareil **suiveur** correspondant. Ceux-ci comprennent les tableaux affichés sous les onglets **Policy Analysis** (Analyse des politiques) et **Enforcement** (Mise en application). Sur l'appareil **leader** (chef de file), cliquez sur **View Charts on Local Appliance** (Afficher les graphiques sur l'appareil local) pour accéder à l'appareil **follower** (suiveur) correspondant.

Illustration 569 : Analyse des politiques sur le chef de file

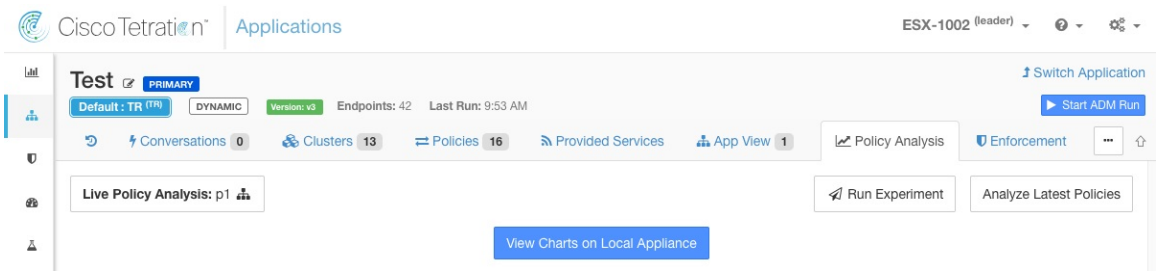
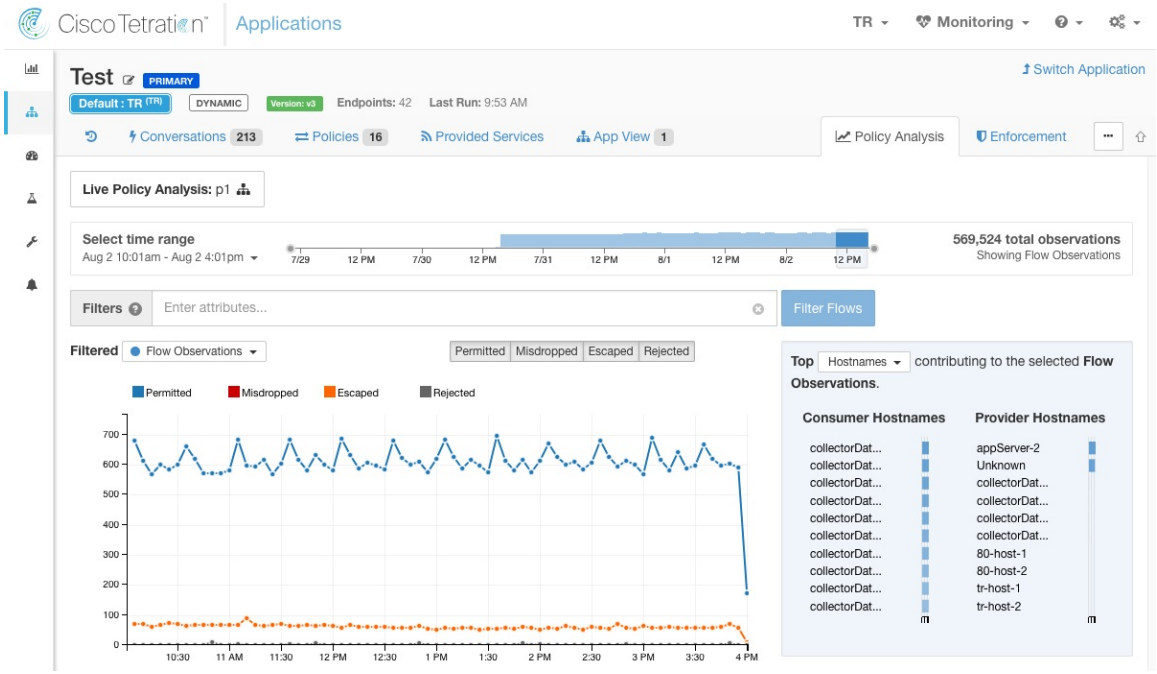
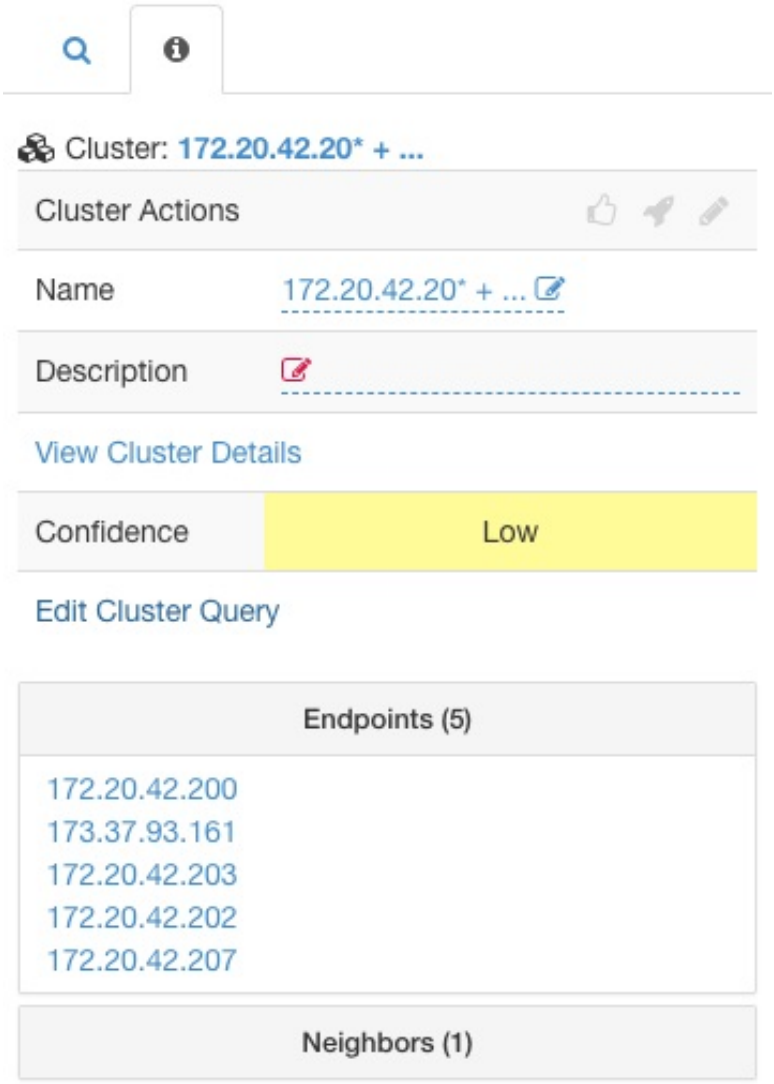


Illustration 570 : Analyse des politiques sur le suiveur



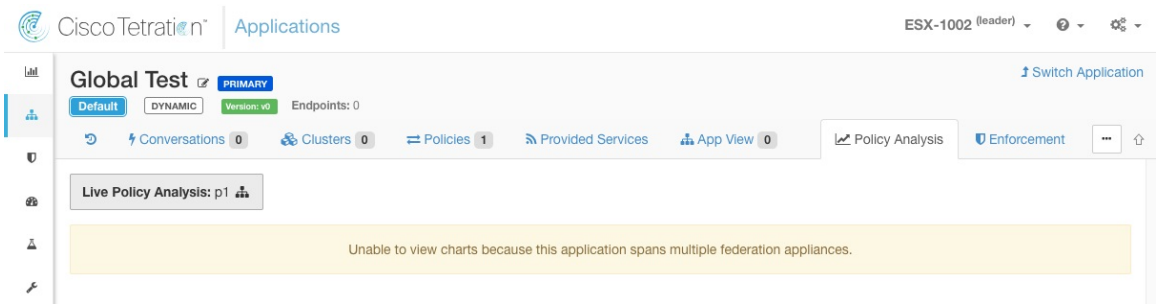
En outre, les recherches dans l'inventaire (à l'exception de la page de découverte automatique des politiques) sont toujours effectuées localement. Par conséquent, il est nécessaire d'accéder au **suiveur** pour afficher les points de terminaison de la grappe, du filtre et de la portée. La même logique s'applique à l'affichage des détails de la grappe, du filtre et de la portée.

Illustration 571 : Panneau latéral de la grappe



Comme expliqué ci-dessus, les espaces de travail créés sur des portées globales ne peuvent pas être utilisés pour la découverte ou l'analyse automatique des politiques. Bien que les politiques puissent être appliquées, les tableaux d'application basés sur les flux ne sont pas disponibles.

Illustration 572 : Analyse des politiques désactivée pour les portées globales



Avertissement Les politiques utilisant un filtre de portée ou d'inventaire restreint associé à un appareil ne seront appliquées que sur cet appareil.

Agents logiciels

Tous les agents logiciels connectés à n'importe quel appareil de la Fédération sont visibles sur le **leader** (chef de file).

Procédure

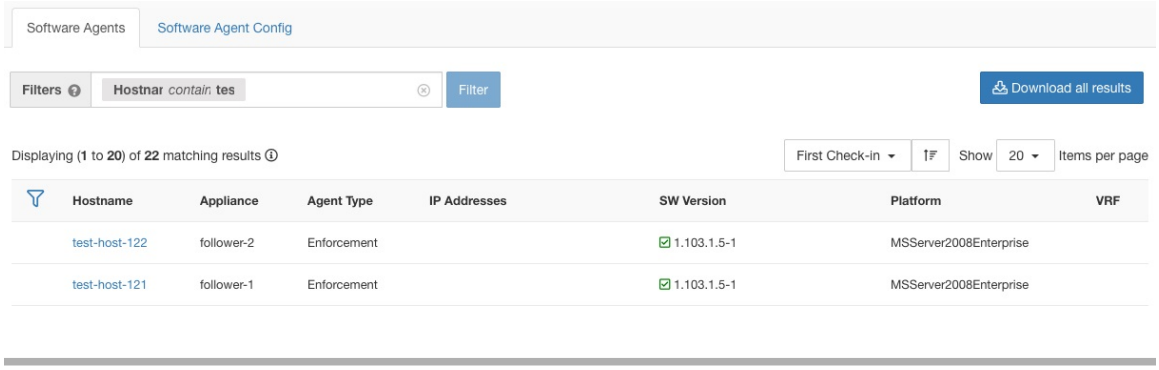
Étape 1 Cliquez sur le **Settings menu** (menu Paramètres) dans le coin supérieur droit.

Étape 2 Sélectionnez **Agent Config** (Configuration de l'agent).
La page **Agent Config** (Configuration de l'agent) s'affiche.

Étape 3 Cliquez sur l'onglet **Software Agents** (Agents logiciels).
L'onglet **Software Agents** (agents logiciels) s'ouvre.

Étape 4 Recherchez un ou plusieurs agents à déplacer et cochez les cases correspondant aux lignes du tableau.

Étape 5 La colonne **Appliance** (Appareil) indique l'endroit où l'agent est connecté.



Déplacement d'agents logiciels entre appareils suiveurs

Les agents logiciels peuvent être déplacés entre les appareils **suiveurs**. À partir de l'appareil auquel l'agent ou les agents sont connectés, procédez comme suit :

Procédure

Étape 1 Cliquez sur le **Settings menu** (menu Paramètres) dans le coin supérieur droit.

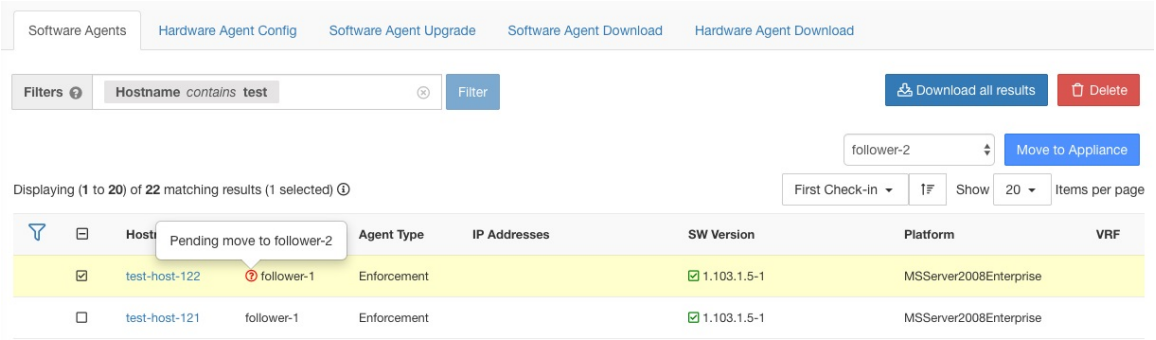
Étape 2 Sélectionnez **Agent Config**(Configuration de l'agent). La page s'affiche.

Étape 3 Cliquez sur l'onglet **Software Agents** (Agents logiciels). L'onglet **Software Agents** (agents logiciels) s'ouvre.

Étape 4 Recherchez un ou plusieurs agents à déplacer et cochez les cases correspondant aux lignes du tableau.

Étape 5 Dans la liste déroulante **-Select Appliance-** (sélectionner un appareil), sélectionnez l'appareil souhaité pour ces agents.

Étape 6 Cliquez sur le bouton **Move to Appliance** (Déplacer vers l'appareil).



Le tableau est mis à jour pour indiquer qu'un déplacement est en attente. Lors de la prochaine connexion de l'agent, il recevra un message l'invitant à déplacer les appareils. Une fois le déplacement terminé, l'agent ne sera plus visible sur l'appareil d'origine. Visiter la page des**Softxare Agents** (agents logiciels) du nouvel appareil pour vérifier que le déplacement a réussi.

Autres tâches

En général, les requêtes basées sur les flux et l'inventaire doivent être effectuées sur les appareils **suiveurs**. Le tableau suivant indique le type d'appareil pour quelques tâches courantes.

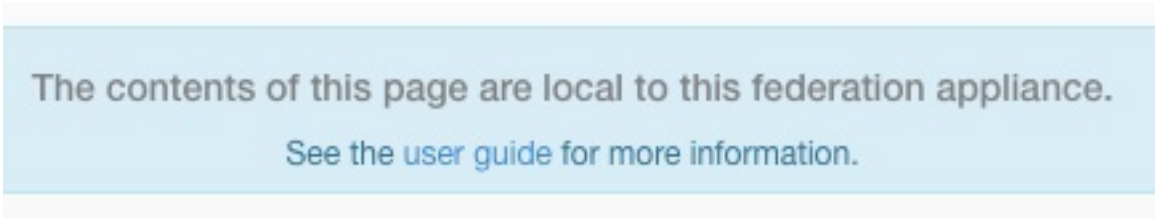
Tableau 50 : Type d'appareil de Fédération pour les tâches courantes

Tâche	Appareil
Visibilité > > **Recherche de flux**	Suiveurs
Visibilité > **Recherche d'inventaire**	Suiveurs
Visibilité > **Filtres d'inventaire**	Suiveurs
Visibilité > **Orchestrateurs externes**	Suiveurs
Segmentation > **Découverte automatique des politiques**	Chef de file
Segmentation > **Analyse des politiques**	Chef de file
Segmentation > **Historique de l'application**	Chef de file

Tâche	Appareil
Segmentation > **Conversations**	Suiveurs
Segmentation > **Résultats de l'analyse**	Suiveurs
Segmentation > **Résultats de l'application**	Suiveurs
Surveillance > **Agents**	Suiveurs
Surveillance > **État d'application**	Suiveurs
Surveillance > **Licences**	Suiveurs
Agents logiciels > **Modifier les appareils**	Suiveurs

Toutes les autres tâches non incluses ci-dessus doivent être considérées comme *locales* à l'appareil. Par conséquent, toutes les modifications apportées ou les résultats affichés ne représentent que l'état de l'appareil actuel, et non l'état de la Fédération. Sur ces pages, l'alerte suivante s'affichera.

Illustration 573 : Alerte d'appareil local



Déploiement existant

Les sections suivantes fournissent un ensemble de directives pour la conservation des données sur les appareils qui rejoignent une Fédération.

Données conservées

L'utilisateur est responsable de la copie des utilisateurs, des rôles, des règles de collecte, des profils criminalistiques, des étiquettes téléversées par l'utilisateur et des configurations d'agent du follower (suiveur) vers le leader (chef de file) avant de l'ajouter à une Fédération. Les données du suiveur qui ne sont pas copiées sur le chef de file sont effacées et remplacées par les données du chef de file.

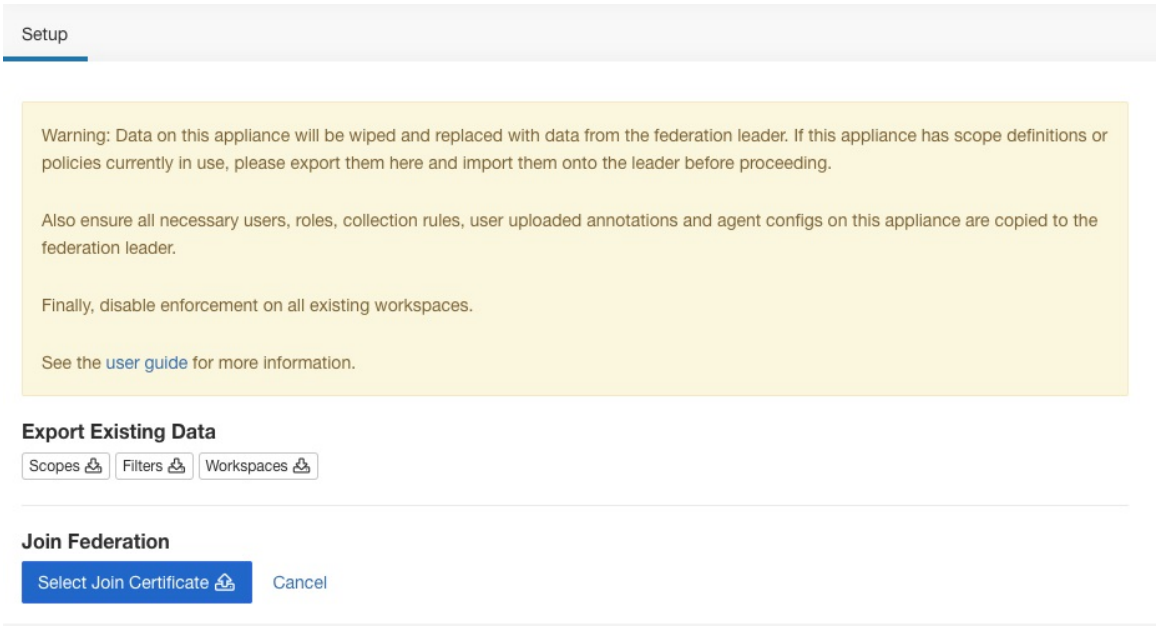
Effectuez les actions suivantes pour préserver les portées, les filtres et les politiques sur les **suiveurs** en les exportant vers des fichiers qui peuvent ensuite être importés sur le **chef de file**.

Procédure

Étape 1 Sur l'appareil suiveur, accédez à **Platform (Plateforme)** > **Federation (Fédération)** et cliquez sur le bouton **Join New Federation** (Rejoindre une nouvelle Fédération).

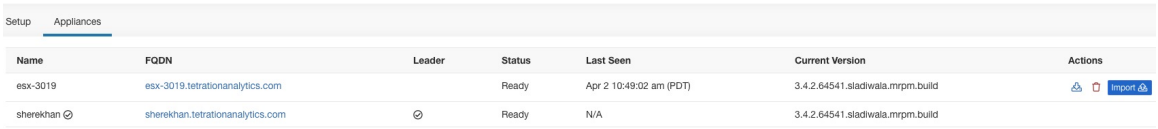
Téléchargez les portées, les filtres et les espaces de travail localement sur l'appareil.

Illustration 574 : Flux de travail d'exportation de déploiement existant sur l'appareil suiveur



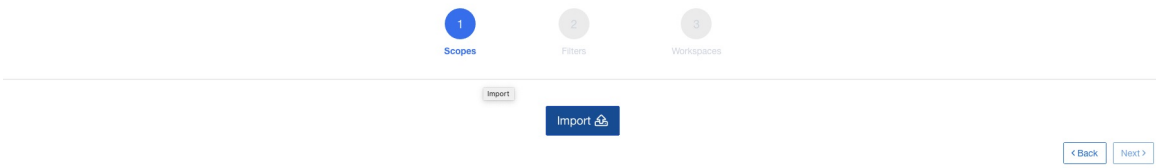
Étape 2 Sur le **chef de file**, accédez à **Platform (Plateforme)** > **Federation (Fédération)**. Ajoutez le suiveur en saisissant son nom et son nom de domaine complet (FQDN) et en cliquant sur le bouton **Add** (ajouter). Passez ensuite à la vue des appareils et cliquez sur le bouton **Import** (Importer) à droite du nom de domaine complet de l'appareil.

Illustration 575 : Icône Importation de déploiement existant sur le suiveur



Vous pouvez charger des portées , des filtres et des espaces de travail téléchargés à partir du suiveur. À chaque étape, résolvez tout conflit avant de passer à l'étape suivante.

Illustration 576 : Assistant d'importation de déploiement existant sur le suiveur



Les conflits entre les entrées sur le chef de file et le suiveur sont détectés en comparant les noms de ces entrées sur les deux appareils. Par exemple, considérons une portée **Default:host** qui existe à la fois sur le chef de file et le suiveur. Sur l'appareil chef de file, la requête pour cette portée est définie sur **Hostname eq foo** et sur l'appareil suiveur, il s'agit de **Hostname eq bar**. L'assistant d'importation avertit l'utilisateur qu'un conflit existe pour cette portée et choisit la requête du chef de file(c'est-à-dire **Hostname eq foo**).

Étape 3 Enfin, vous devez *désactiver la mise en application* sur tous les espaces de travail existants sur le suiveur avant de l'ajouter à la Fédération.

Étape 4 Les étapes 1 à 3 doivent être répétées pour chaque appareil suiveur qui rejoint la Fédération.

Données non conservées

1. Les appliances virtuelles (y compris celles utilisées avec les connecteurs) doivent être remises en service sur un appareil suiveur après qu'il ait rejoint la Fédération.
2. Les données de flux sur un suiveur jusqu'au moment où il rejoint la Fédération sont inaccessibles pour les portées communes avec le chef de file.

Mode de fonctionnement déconnecté

Remarque Applicable aux suiveurs.

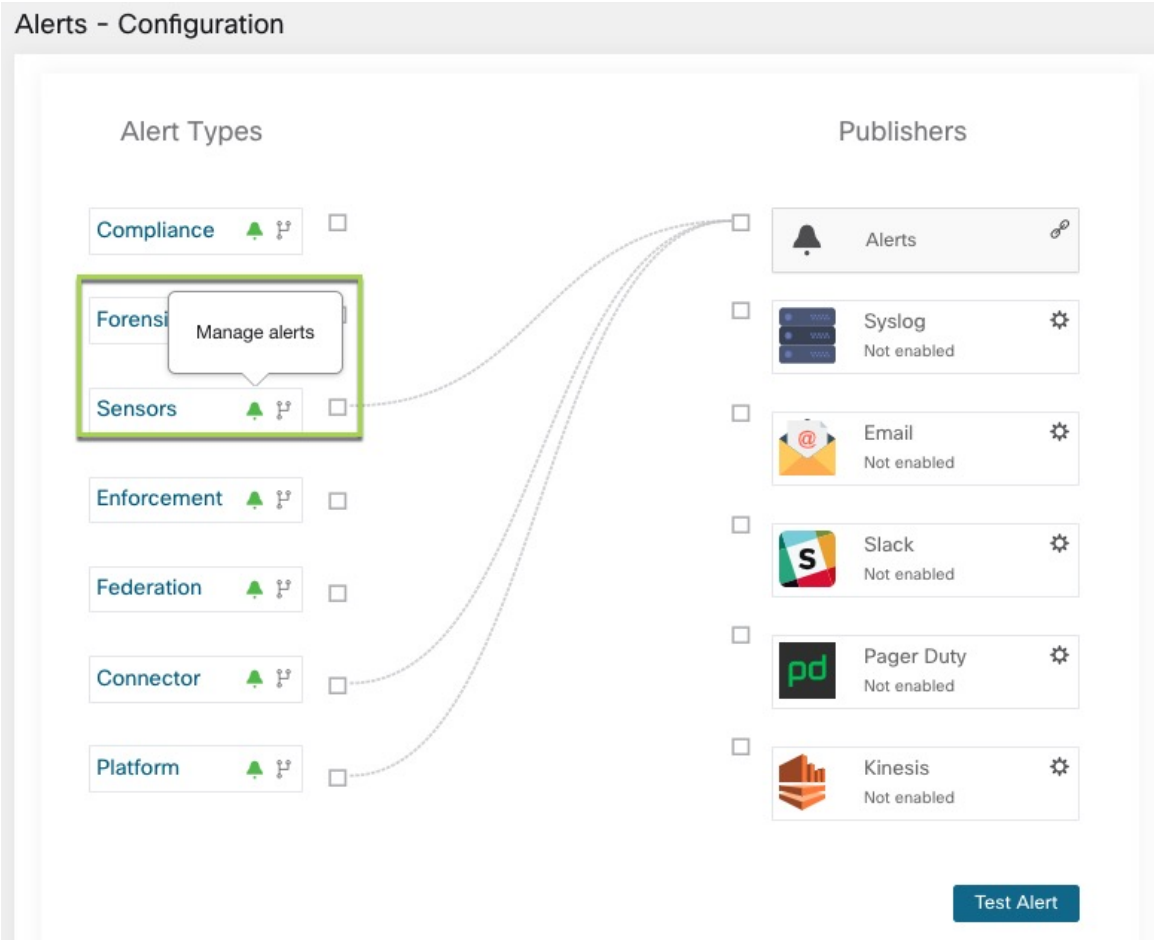
Dans certaines circonstances, par exemple en cas de partition réseau, il est logique de désactiver la Fédération sur un ou plusieurs **suiveurs**, ce qui leur permet de fonctionner en mode autonome. Pour ce faire, accédez à **Platform** (plateforme **)** et cliquez sur le bouton **Disable** (désactiver). Un suiveur qui est déconnecté de la Fédération continue de fonctionner en tant que grappe autonome.

Les nouvelles portées, les filtres d'inventaire et les espaces de travail du suiveur peuvent être préservés en les exportant vers des fichiers qui sont ensuite importés sur le leader (chef de file) avant de le réintégrer dans la Fédération. Cela conserve les modifications apportées aux politiques pour les espaces de travail existants. Cependant, les modifications apportées aux portées et aux filtres d'inventaire déjà présents sur le leader sont perdues lorsque le suiveur rejoint la Fédération.

Configurer les alertes

Pour activer les alertes, dans le volet de navigation, choisissez **Manage** > **Workloads** > **Alert Configs** (Gestion > Charges de travail > Configurations des alertes). Mettre à jour la configuration des alertes pour la Fédération

Illustration 577 : Alertes de la Fédération



Vous pouvez générer des alertes pour les événements suivants :

- Générez des alertes sur le contrôleur chef de file de niveau de gravité MOYENNE lorsqu'un ou plusieurs appareils de la Fédération n'ont pas été en contact avec lui depuis plus de 10 minutes.
- Générer des alertes sur le suiveur avec un niveau de gravité MOYENNE lorsqu'il ne peut pas contacter le contrôleur chef de file pendant plus de 10 minutes.

Détails de l'alerte

Consultez Structure commune des alertes, à la page 693 pour obtenir la structure générale des alertes et des informations sur les champs. Le champ *alert_détails* est structuré et contient les sous-champs suivants pour les alertes de Fédération

Remarque *Appliance*, il s'agit de l'appareil qui a déclenché l'alerte.

Tableau 51 : Détails de l'alerte de Fédération

Champ	Type d'alerte	Format	Explication
ID	*tous*	chaîne	ID de dispositif
Nom	*tous*	chaîne	Nom de l'appareil
fqdn	*tous*	chaîne	Nom de domaine complet (FQDN) de l'appareil
is_leader	*tous*	booléen	True (vrai) si l'appareil est le leader (chef de file)
état	*tous*	chaîne	État de l'appareil
current_sw_version	*tous*	chaîne	Version du logiciel sur l'appareil
last_seen_at	*tous*	nombre entier	Horodatage Unix du moment où l'appareil a été vu pour la dernière fois
created_at	*tous*	nombre entier	Horodatage Unix de la création de l'appareil
updated_at	*tous*	nombre entier	Horodatage Unix de la mise à jour de l'appareil
created_at	*tous*	nombre entier	Horodatage Unix de la création de l'appareil
deleted_at	*tous*	nombre entier	Horodatage Unix de la suppression de l'appareil.
disconnected	*tous*	booléen	Défini à « vrai » lorsque l'abonné s'est déconnecté du leader. Toujours mettre à « faux » pour le leader

Exemple de alert_détails pour une alerte de suiveur déconnecté

```
{
  "id": "5f219ad8755f024b46c2524a",
  "name": "esx-3018",
  "fqdn": "esx-3018.tetrationanalytics.com",
  "is_leader": false,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": true
}
```

Exemple de alert_details pour une alerte de leader déconnecté

```
{
  "id": "5f219acc755f024b46c25248",
  "name": "sherekhan",
  "fqdn": "sherekhan.tetrationanalytics.com",
  "is_leader": true,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": false
}
```


API

Remarque Les renseignements d'authentification pour une grappe de Fédération doivent être générés sur le chef de file et peuvent être utilisés pour interroger les suiveurs.

Cette section répertorie les API ajoutées ou mises à jour pour la Fédération :

Appareils

Le point terminal des appareils permet à l'utilisateur de récupérer l'état d'un appareil dans une Fédération.

Objet appareil

Les attributs de l'objet appareil sont décrits dans le tableau suivant :

Attribut	Type	Description
ID	chaîne	Identifiant unique pour l'appareil.
name	chaîne	Nom précisé par l'utilisateur pour l'appareil.
fqdn	chaîne	Nom de domaine complet (FQDN) de l'appareil spécifié par l'utilisateur.
is_leader	booléen	Indique si l'appareil est un leader (chef de file).
état	chaîne	État de l'appareil.
current_sw_version	chaîne	Version du logiciel Cisco Secure Workload sur l'appareil.
last_seen_at	nombre entier	Horodatage Unix du moment où le suiveur a été vu pour la dernière fois par le leader. Il est toujours nul pour le leader.

Attribut	Type	Description
deleted_at	nombre entier	Horodatage Unix de la suppression de l'appareil.
disconnected	booléen	Indique si le suiveur a perdu le contact avec le leader. La valeur est faux pour le leader.

Répertorier les appareils

Ce point terminal renvoie un tableau d'appareils dans le regroupement Fédération.

```
GET /openapi/v1/appliances
```

Paramètres : Aucun

Objet de réponse : renvoie un tableau des objets de l'appareil.

Exemple de code Python

```
restclient.get('/appliances')
```

Portées

Le Objet portée, à la page 996 comprend maintenant l'ID de l'appareil associé à une portée. Il est défini à null pour les portées globales.

Les API suivantes acceptent maintenant un ID d'appareil lors de la création ou de la mise à jour des portées.

Créer une portée

Un ID d'appareil fourni lors de la création d'une portée l'associe à un appareil spécifique.

```
POST /openapi/v1/app_scopes
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.
parent_app_scope_id	chaîne	ID de la portée parente.
policy_priority	nombre entier	La valeur par défaut est « dernier ». Utilisé pour trier les priorités de l'espace de travail. Voir le classement des politiques sous Consulter les politiques découvertes automatiquement, à la page 538.

Nom	Type	Description
appliance_id	chaîne	Identifiant unique pour l'appareil.

Exemple de code Python

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "parent_app_scope_id": <parent_app_scope_id>,
    "appliance_id": <appliance_id>,
}
resp = restclient.post('/app_scopes', json_body=json.dumps(req_payload))
```

Mettre à jour une portée

Cette API permet d'associer des portées existantes à des appareils en utilisant leur ID d'appareil.

```
PUT /openapi/v1/app_scopes/{app_scope_id}
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.
appliance_id	chaîne	Identifiant unique pour l'appareil.

Renvoie l'objet de portée modifié associé à l'ID spécifié.

Exemple de code Python

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "appliance_id": <appliance_id>,
}
resp = restclient.put('/app_scopes/%s' % <app_scope_id>,
                      json_body=json.dumps(req_payload))
```

Session inactive

Pour ceux qui s’authentifient à l’aide d’une base de données locale, cette section explique comment des tentatives de connexion infructueuses peuvent verrouiller le compte d’utilisateur :

Procedure

Étape 1 Cinq tentatives infructueuses de connexion à l’aide d’une adresse de courriel et d’un mot de passe entraînent le verrouillage du compte.

Note Par mesure de sécurité contre les tentatives de connexion malveillantes, aucun message précis indiquant le verrouillage ne s’affichera dans l’interface de connexion lorsque vous tenterez de vous connecter à un compte verrouillé.

Étape 2 La durée du verrouillage est de 30 minutes. Une fois le compte déverrouillé, utilisez le mot de passe correct pour vous connecter ou lancez la récupération du mot de passe en cliquant sur *Mot de passe oublié?*

Note Une fois que l'utilisateur s'est connecté avec succès, il est déconnecté après une heure d'inactivité. Ce délai d’expiration est configuré à partir de **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Session Configuration (Configuration de session)**.

Préférences

La page **Preferences** (Préférences) affiche les détails de votre compte et vous permet de mettre à jour vos préférences d’affichage, de modifier votre page de destination, de modifier votre mot de passe et de configurer l’authentification à deux facteurs.

Modifier vos préférences de page de destination

Pour modifier la page qui s’affiche lorsque vous vous connectez :

Procedure

Étape 1 Dans le coin supérieur droit de la fenêtre, cliquez sur l’icône d’utilisateur et choisissez **User Preferences** (Préférences de l’utilisateur).

Étape 2 Choisissez une page de destination dans le menu déroulant. Vos préférences sont enregistrées comme page d’accueil ou par défaut lorsque vous vous connectez. Pour afficher la modification, cliquez sur le logo Cisco Secure Workload dans le coin supérieur gauche de la page.

Modification d'un mot de passe

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Dans le volet **Change Password** (modifier le mot de passe), saisissez votre mot de passe actuel dans le champ **Old Password** (Ancien mot de passe).

Étape 4 Saisissez votre nouveau mot de passe dans le champ **Password** (Mot de passe).

Étape 5 Saisissez votre nouveau mot de passe dans le champ **Password** (Mot de passe).

Étape 6 Cliquez sur **Change Password** (modifier le mot de passe) pour soumettre la modification.

Note **Le mot de passe doit comporter entre 8 et 128 caractères et contenir au moins un des éléments suivants :**

- Lettres minuscules (a b c d . . .)
- Lettres majuscules (A B C D . . .)
- Chiffres (0 1 2 3 4 5 6 7 8 9)
- Caractères spéciaux (! " # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ' { | } ~), espace compris

Récupération des mots de passe

Cette section explique comment récupérer votre mot de passe.

Before you begin

Pour réinitialiser un mot de passe, vous devez d’abord avoir un compte. Un nouveau compte peut être ajouté par les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle**.

Procedure

Étape 1 Pointez votre navigateur sur l’URL Cisco Secure Workload de Cisco et cliquez sur le lien **Mot de passe oublié**. La boîte de dialogue **Mot de passe oublié?** s'affiche.

Étape 2 Saisissez votre adresse courriel dans le champ **Adresse de courriel**.

Étape 3 Cliquez sur **Réinitialiser le mot de passe**.

Des instructions de réinitialisation de mot de passe sont envoyées à votre adresse courriel.

Note La procédure de récupération du mot de passe pour l’authentification à deux facteurs nécessite de contacter le service d'assistance à la clientèle Cisco Secure Workload, car la récupération du mot de passe par courriel ne peut pas contenir le mot de passe à usage unique.

Activation de l'authentification à deux facteurs

Cette section explique comment activer l’authentification à deux facteurs.

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Dans le volet **Two-factor authentication** (Authentification à deux facteurs), cliquez sur le bouton **Enable** (activer). Un nouveau volet **d’authentification à deux facteurs** s’affiche.

Étape 4 Saisissez votre mot de passe.

Étape 5 Balayez le code QR qui s’affiche dans le champ **Current Password** (Mot de passe actuel) à l’aide d’une application de mot de passe à usage unique basé sur le temps (TOTP), comme Google Authenticator (pour Android ou iOS) ou Authenticator (pour Windows Phone).

Étape 6 Saisissez le code de validation affiché par l’application TOTP de votre choix.

Étape 7 Cliquez sur **Enable** (Activer).

Figure 578: Volet Authentification à deux facteurs

La prochaine fois que vous vous connecterez au système, vous devrez cocher la case **Use deux facteurs authentication** (utiliser l'authentification à deux facteurs) et saisir le code de vérification qui s'affiche dans votre application TOTP pour vous connecter.

Note La procédure de récupération du mot de passe pour l'authentification à deux facteurs nécessite de contacter le service d'assistance à la clientèle Cisco Secure Workload, car la récupération du mot de passe par courriel ne peut pas contenir le mot de passe à usage unique.

Désactivation de l'authentification à deux facteurs

Cette section explique comment désactiver l'authentification à deux facteurs.

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Sous Two-factor authentication (Authentification à deux facteurs), cliquez sur le bouton **Disable** (désactiver). Le volet **Authentification à deux facteurs** s'affiche.

Étape 4 Saisissez votre mot de passe.

Étape 5 Cliquez à nouveau sur le bouton **Disable** (désactiver).

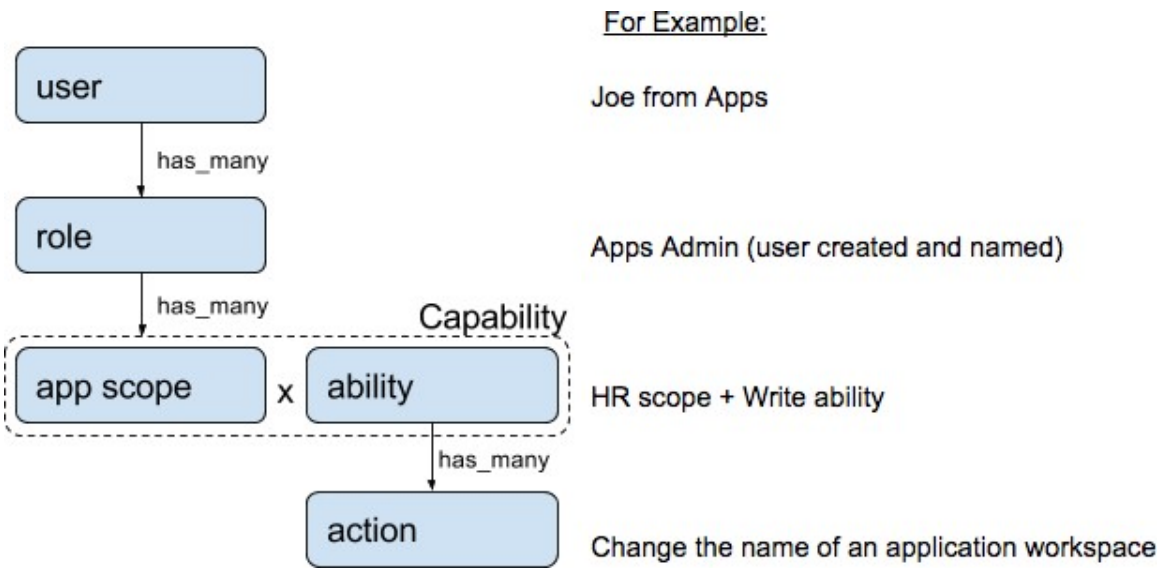
Vous ne serez plus tenu de saisir un code d'authentification à deux facteurs lors de la connexion.

Rôles

Vous pouvez restreindre l'accès aux fonctionnalités et aux données à l'aide du modèle de contrôle d'accès basé sur les rôles (RBAC).

- Utilisateur : personne avec un accès de connexion à Cisco Cisco Secure Workload.
- Rôle : ensemble de capacités créé par l'utilisateur qui est affecté à un utilisateur.
- Capability (Capacité) : couple portée + aptitude
- Ability (Aptitude) : ensembles d'actions
- Action : action de bas niveau de l'utilisateur, comme « modifier le nom de l'espace de travail »

Figure 579: Modèle de rôle



Un utilisateur peut avoir n'importe quel nombre de rôles. Les rôles peuvent avoir un nombre illimité de capacités. Par exemple, le rôle « Ingénieur de recherche en ressources humaines » pourrait avoir deux capacités :

« Lire sur la portée des ressources humaines » pour donner de la visibilité et du contexte et « Exécuter dans la fonctionnalité « Recherche RH » pour permettre aux ingénieurs ayant ce rôle d'apporter des modifications précises qui sont nécessaires. liées à leurs demandes.

Les rôles contiennent des ensembles de capacités et sont affectés aux utilisateurs dans la page **Users** (Utilisateurs). Un utilisateur peut avoir n'importe quel nombre de rôles. Les rôles peuvent avoir un nombre illimité de capacités.

Rôle	Description
Programme d'installation de l'agent	Fournir la capacité de gérer le cycle de vie des agents, y compris l'installation, la surveillance, la mise à niveau et la conversion, mais **ne pas pouvoir** supprimer les agents et accéder au profil de configuration de l'agent.
Le service d'assistance à la clientèle	Pour l'assistance technique ou les services avancés. Fournit un accès aux fonctionnalités d'entretien de la grappe. Autorise le même accès que l'administrateur du site, mais **ne peut pas** modifier les utilisateurs.
Le service d'assistance à la clientèle	Pour l'assistance technique ou les services avancés. Fournit un accès aux fonctionnalités d'entretien de la grappe. Autorise le même accès que l'administrateur du site, mais **ne peut pas** modifier les utilisateurs.
Administrateur du site	Offre la possibilité de gérer les utilisateurs, les agents, etc. Peut afficher et modifier toutes les fonctionnalités et toutes les données. Il doit y avoir au moins un administrateur de site.
Mise en application mondiale des applications	Fournit la capacité Mise en application sur chaque portée.
Gestion d'application mondiale	Fournit la capacité d'exécution sur chaque portée.
Lecture seule mondiale	Fournit la capacité de lecture sur chaque portée.

Aptitudes et capacités

Les rôles sont composés de capacités, qui comprennent une portée et une aptitude. Celles-ci définissent les actions autorisées et l'ensemble de données auquel elles s'appliquent. Par exemple, la capacité (RH, Lecture) doit être lue et interprétée comme « Capacité de lecture sur la portée des ressources humaines ». Cette fonctionnalité permet d'accéder à la portée des ressources humaines et à tous ses enfants.

Capacité	Description
Programme d'installation	Installer, surveiller et mettre à niveau les agents logiciels.
Vérification	Prise en charge globale de la lecture des données des appareils et accès aux journaux des modifications.
Lecture	Lire toutes les données, y compris les flux, les filtres d'application et d'inventaire.
Écriture	Apporter des modifications aux applications et aux filtres d'inventaire.
Exécuter	Exécuter Découvrir automatiquement les politiques, exécuter et publier les politiques pour analyse.

Capacité	Description
Appliquer	Appliquez les politiques définies dans les espaces de travail d'application associés à la portée donnée.
Owner (responsable)	Requis pour basculer un espace de travail d'application de secondaire à principal. Accès aux capacités d'administration des dérivations de données, comme la gestion des sessions d'application utilisateur, l'ajout de dérivations de données et la création de sources de données de visualisation.

Important Les capacités sont héritées, par exemple, la capacité d'exécution permet toutes les actions de lecture, d'écriture et d'exécution.

Important Les capacités s'appliquent à la portée et à tous ses enfants.

Accès au menu par rôle

Les menus qu'un utilisateur peut voir et utiliser dépendent du rôle qui lui est attribué :

Table 52: Menu Overview (Aperçu)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Aperçu	Aperçu	Oui	Oui	Oui	Oui	Oui	Non

Table 53: Menu Overview (Aperçu)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Aperçu	Aperçu	Oui	Oui	Oui	Oui	Oui	Oui	Non
Création de rapports	Aperçu	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 54: Menu Organize (Organiser)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Organiser	Portées et inventaire	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Utiliser les étiquettes téléversées	Oui	Oui	Non	Non	Non	Non
Organiser	Filtres d'inventaire	Oui	Oui	Oui	Oui	Oui	Non

Table 55: Menu Organize (Organiser)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Organiser	Portées et inventaire	Oui	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Gestion des étiquettes	Oui	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Filtres d'inventaire	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 56: Menu Defend (Défendre)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Défendre	Segmentation	Oui	Oui	Oui	Oui	Non	Non
Défendre	État d'application	Oui	Oui	Non	Non	Non	Non
Défendre	Modèles de politiques	Oui	Oui	Non	Non	Non	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Défendre	Règles criminalistiques	Oui	Oui	Non	Non	Non	Non

Table 57: Menu Defend (Défendre)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Défendre	Segmentation	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	État d'application	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	Modèles de politiques	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	Règles criminalistiques	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 58: Menu Investigate (Enquêter)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Analyse	Trafic	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Alertes	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Vulnérabilités	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Criminalistique	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Quartier	Oui	Oui	Oui	Oui	Oui	Non

Table 59: Menu Investigate (Enquêter)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Analyse	Trafic	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Alertes	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Vulnérabilités	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Criminalistique	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 60: Menu Manage (Gestion)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Gérer	Configurations d'alertes	Oui	Oui	Oui	Oui	Oui	Oui	Non
Gérer	Journaux des modifications	Oui	Non	Oui	Non	Non	Non	Non
Gérer	Connecteurs	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Orchestrateurs externes	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Connecteur sécurisé	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Appliances virtuelles	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Utilisateurs	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Rôles	Oui	Oui	Oui	Non	Non	Non	Non
Gérer	Informations sur les menaces	Oui	Oui	Oui	Non	Non	Non	Non
Gérer	Licences	Oui	Non	Non	Non	Non	Non	Non
Gérer	Règles de collecte	Oui	Oui	Oui	Oui	Oui	Oui	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Gérer	Configuration de session	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Analyse de l'utilisation	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Administrateur de surveilleur de données	Oui	Non	Non	Non	Non	Non	Non

Table 61: Menu Platform (Plateforme)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Observations	Détenteurs	Oui	Oui	Non	Non	Non	Non	Non
Observations	Configuration de grappe	Oui	Oui	Non	Non	Non	Non	Non
Observations	HTTP sortant	Oui	Oui	Non	Non	Non	Non	Non
Observations	Collecteurs	Oui	Oui	Non	Non	Non	Non	Non
Observations	Authentification extérieure	Oui	Oui	Non	Non	Non	Non	Non
Observations	Certificat SSL	Oui	Oui	Non	Non	Non	Non	Non
Observations	Message de page de connexion	Oui	Oui	Non	Non	Non	Non	Non
Observations	Fédération	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Observations	Sauvegarde des données	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Observations	Restauration des données	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Observations	Mise à niveau automatique	Oui	Oui	Non	Non	Non	Non	Non

Note

- L'option Fédération est accessible pour les rôles d'administrateur du site et de service d'assistance à la clientèle si la Fédération est activée.
- Les options de sauvegarde et de restauration des données sont accessibles aux administrateurs du site et aux rôles de service d'assistance à la clientèle si la sauvegarde et la restauration des données sont activées.

Table 62: Menu Troubleshoot (Dépannage)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Dépanner	État du service	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	État de la grappe	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Dépanner	Machine virtuelle	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	Instantanés	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Explorateur de maintenance	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Resque	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Hawkeye (Graphiques)	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	Abyss (Pipeline)	Oui	Oui	Oui	Non	Non	Non	Non

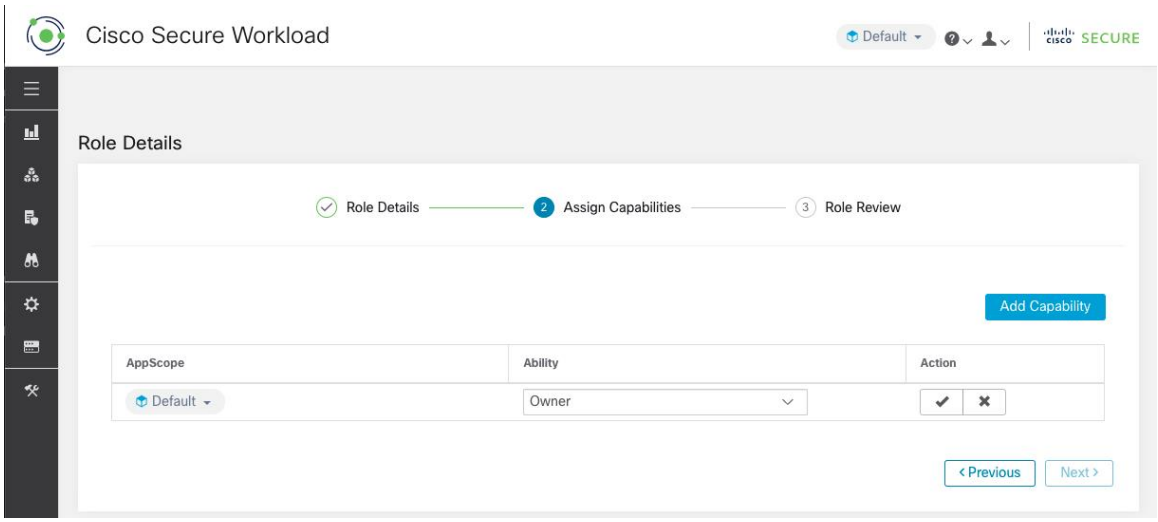
Note L'option État de la grappe est accessible aux administrateurs du site et aux rôles de service d'assistance à la clientèle selon le type de grappe.

Créer un rôle

Before you begin

Vous devez déjà avoir un rôle d' **administrateur du site** ou de service d'assistance à la clientèle.

1. Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Roles (Rôles)** .
2. Cliquez sur **Create New Role** (Créer un nouveau rôle). Le panneau **Roles** (Rôles) s'affiche.



La création d'un rôle à l'aide de l'assistant de création de rôle est un processus en trois étapes.

Procedure

Étape 1 a) Saisissez les valeurs appropriées dans les champs suivants :

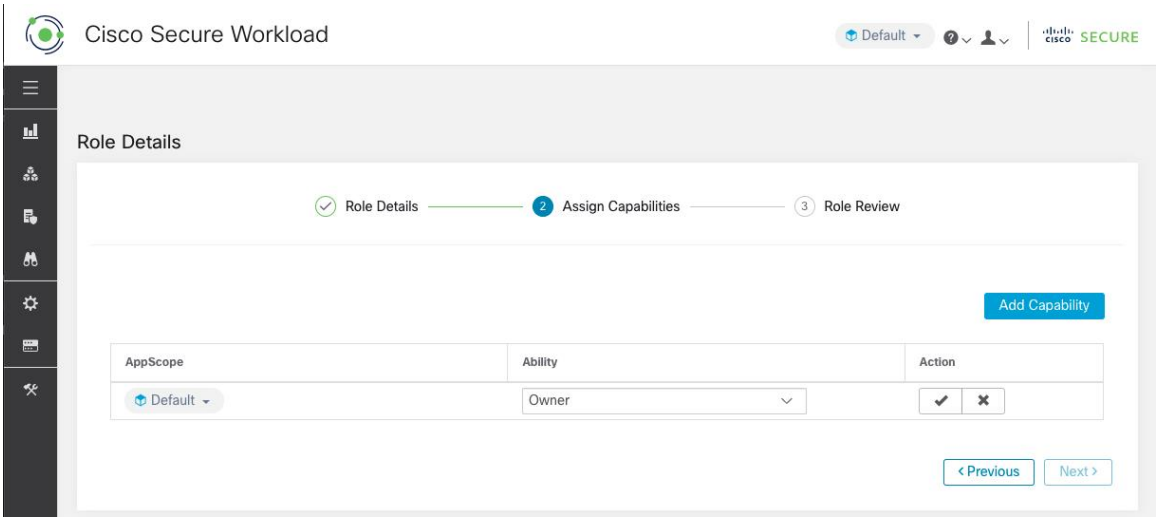
Champ	Description
Nom	Le nom pour identifier le rôle.
Description	Une brève description du rôle pour ajouter du contexte.

b) Cliquez sur le bouton **Next** (suivant) pour passer à l'étape suivante ou sur **Back to Roles Page** pour revenir à la page des rôles.

Étape 2 a) Cliquez sur le bouton **Add Capability** (ajouter une capacité) pour afficher le formulaire de création dans la rangée supérieure.

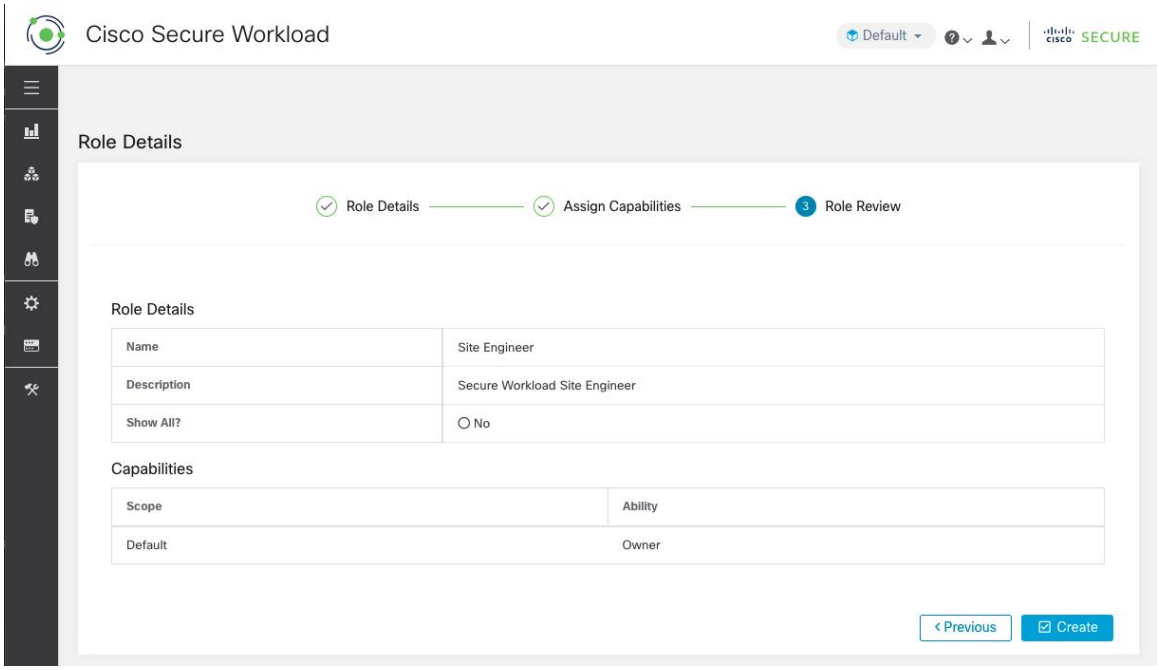
b) Sélectionnez la portée et la fonctionnalité.
c) Cliquez sur le bouton **Checkmark** (Coche) pour créer une nouvelle capacité ou sur le bouton **Cancel** (Annuler) pour annuler.
d) Cliquez sur **Next** (suivant) pour consulter les détails du rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier.

Figure 580: Affectation de capacité



Étape 3
a) Passez en revue les détails et les capacités du rôle.
b) Cliquez sur **Create** (créer) pour créer un rôle.

Figure 581: Examen du rôle



Modifier un rôle

Cette section explique comment les **administrateurs de site** et **les utilisateurs du service d'assistance à la clientèle** peuvent modifier des rôles.

Before you begin

Vous devez être l'administrateur du site ou l'utilisateur du service d'assistance à la clientèle.

1. Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Roles (Rôles)** .
2. Sur la ligne du rôle à modifier, cliquez sur le bouton **Edit** (modifier) dans la colonne de droite. Le panneau **Roles** (Rôles) s'affiche.

La modification d'un rôle à l'aide de l'assistant de modification de rôle est un processus en trois étapes.

Procedure

Étape 1

a) Mettez à jour le nom ou la description si vous le souhaitez.
b) Cliquez sur le bouton **Next** (suivant) pour passer à l'étape suivante ou sur **Back to Roles Page** pour revenir à la page des rôles.

Étape 2

a) Supprimez une capacité le cas échéant. Sur la ligne représentant la capacité à supprimer, cliquer sur l'icône **Delete** (Supprimer) dans la colonne de droite.

b) Pour en ajouter, une cliquez sur le bouton **Add Capability** (Ajouter une capacité) afin d'afficher le formulaire de création dans la rangée supérieure.
c) Sélectionnez la portée et la fonctionnalité.
d) Cliquez sur **Next** (suivant) pour consulter les détails du rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier.

Étape 3

a) Passez en revue les détails et les capacités du rôle.
b) Cliquez sur **Update** (Mettre à jour) pour créer le rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier. Les modifications apportées aux détails du rôle et à l'attribution des capacités sont enregistrées après la **mise à jour**.

Note Les capacités ne peuvent pas être modifiées, elles doivent être supprimées et recréées.

Portées

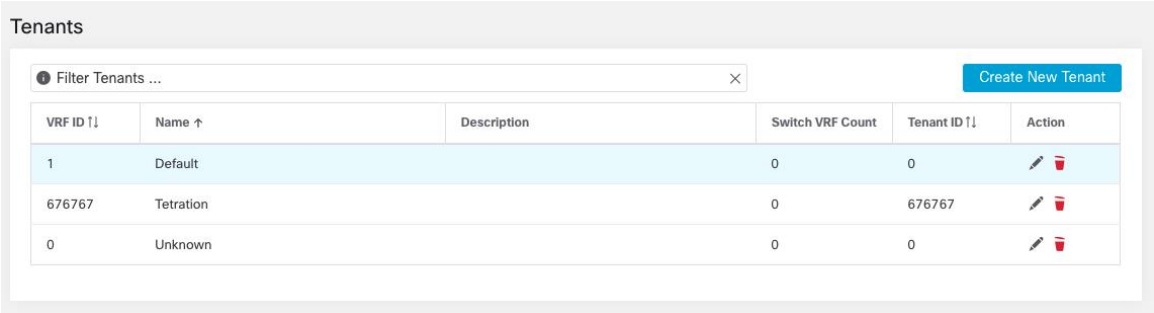
Note La page **Scopes** (Portées) est fusionnée avec **Inventory Search** (Recherche dans l'inventaire). (Pour obtenir de plus amples renseignements, consultez la page Portées et inventaire (Portées et inventaire).

Détenteurs

Les **administrateurs du site** et les **utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Tenants** (Détenteurs) dans le menu **Platform (Plateforme)** > **Tenants** (Détenteurs) dans le volet de navigation de gauche. La page Tenants (Détenteurs) affiche les détenteurs et les VRF actuellement configurés Cisco Secure Workload est préconfiguré avec un ou plusieurs détenteurs et VRF, et vous pouvez ajouter, modifier et supprimer des détenteurs.

Note Ces valeurs affectent les résultats de la sortie de la grappe. Nous vous recommandons de consulter le service d'assistance technique Cisco TAC avant de modifier ces valeurs pour comprendre l'incidence sur le système.

Figure 582: Page Tenants (Détenteurs)



Ajouter un détenteur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur du **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Platform(Plateforme)** > **Tenants (Détenteurs)** .

Étape 2 Cliquez sur **Créer un nouveau détenteur**.

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Saisissez le nom souhaité pour le détenteur.
Description	(Facultatif) Le champ de description contient des informations supplémentaires sur le détenteur.

Étape 4 Cliquez sur **Create** (créer).

Modifier un détenteur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur du **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Platform(Plateforme)** > **Tenants (Détenteurs)** .

Étape 2 Recherchez le locataire que vous souhaitez modifier et cliquez sur l'icône en forme de **crayon** dans la colonne de droite.

Champ	Description
Nom	Saisissez un nom pour le détenteur.
Description	(Facultatif) Mettez à jour le champ de description qui contient des informations supplémentaires sur le détenteur.
ID VRF	Affiche l'ID de ce détenteur ou VRF particulier.
Journal des modifications	Cliquez sur les icônes du journal des modifications pour afficher une nouvelle page qui affiche le journal des modifications pour le détenteur ou VRF.

Étape 3 Cliquez sur **Update** (mettre à jour).

Utilisateurs

Les administrateurs du site et les propriétaires de portée racine peuvent accéder à la page **Users** (Utilisateurs) dans le menu **Manage(Gestion)** > **User Access (Accès des utilisateurs)** dans la barre de navigation à gauche de la fenêtre.

Cette page affiche tous les utilisateurs du fournisseur de services et les utilisateurs associés à la portée dans l'en-tête de page.

Multidétenteurs

Pour prendre en charge l'architecture à détenteurs multiples, affectez les utilisateurs à une portée racine. Les utilisateurs disposant de la capacité « Propriétaire » sur la portée racine gèrent ces utilisateurs et attribuent des rôles qui sont associés à la même portée.

Les fournisseurs de services sont des utilisateurs sans portée; affectez un rôle leur permettant d'effectuer des actions dans plusieurs portées racine.

Ajouter un utilisateur

Before you begin

- Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée** pour ajouter des utilisateurs à Cisco Secure Workload.
- Si une portée multi-détenteurs est attribuée à un utilisateur, seuls les rôles attribués à la même portée peuvent être sélectionnés.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Le cas échéant, sélectionnez la portée racine appropriée dans l'en-tête de page.

Étape 2 Dans le volet de navigation, choisissez **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 3 Cliquez sur **Create New User** (Créer un nouvel utilisateur).
La page **User Details** (des détails de l'utilisateur) s'affiche.

Étape 4 Mettez à jour les champs suivants sous **User Details** (Détails sur l'utilisateur) .

Table 63: Description des champs des détails de l'utilisateur

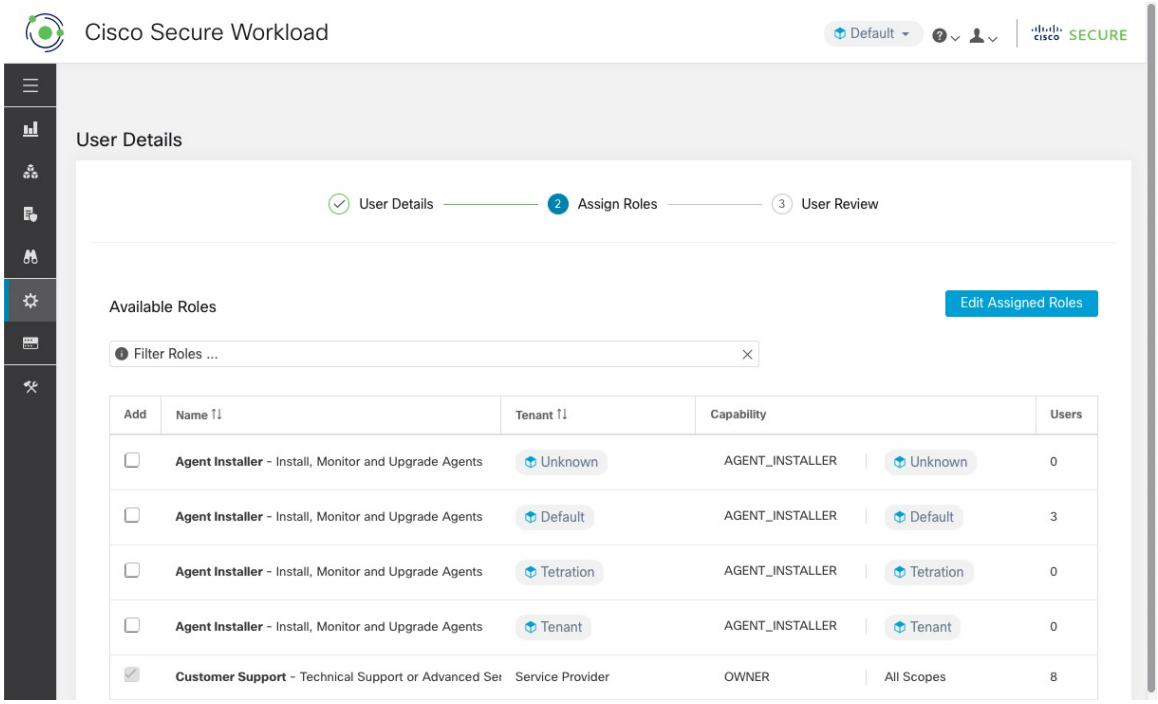
Champ	Description
Email	Saisissez l'identifiant de courriel de l'utilisateur. Il n'est pas sensible à la casse. Nous utilisons la version en lettres minuscules de votre courriel s'il contient des lettres.
Prénom	Saisissez le prénom de l'utilisateur.
Nom	Saisissez le nom de famille de l'utilisateur.
Scope	La portée racine qui est affectée à l'utilisateur pour l'architecture multidétenteurs. (Disponible pour les administrateurs du site)
Clé publique SSH	(Facultatif) Cliquez sur **Import** (importer) pour importer une clé publique SSH. Vous pouvez également en importer une ultérieurement.

Étape 5 Cliquez sur **Next** (suivant).

Étape 6 Sous **Assign Roles** (Affecter des rôles), ajoutez ou supprimez des rôles attribués à l'utilisateur.

- Cliquez sur **Add rôles** (Ajouter des rôles) pour attribuer de nouveaux rôles, puis cochez la case **Add** (ajouter).

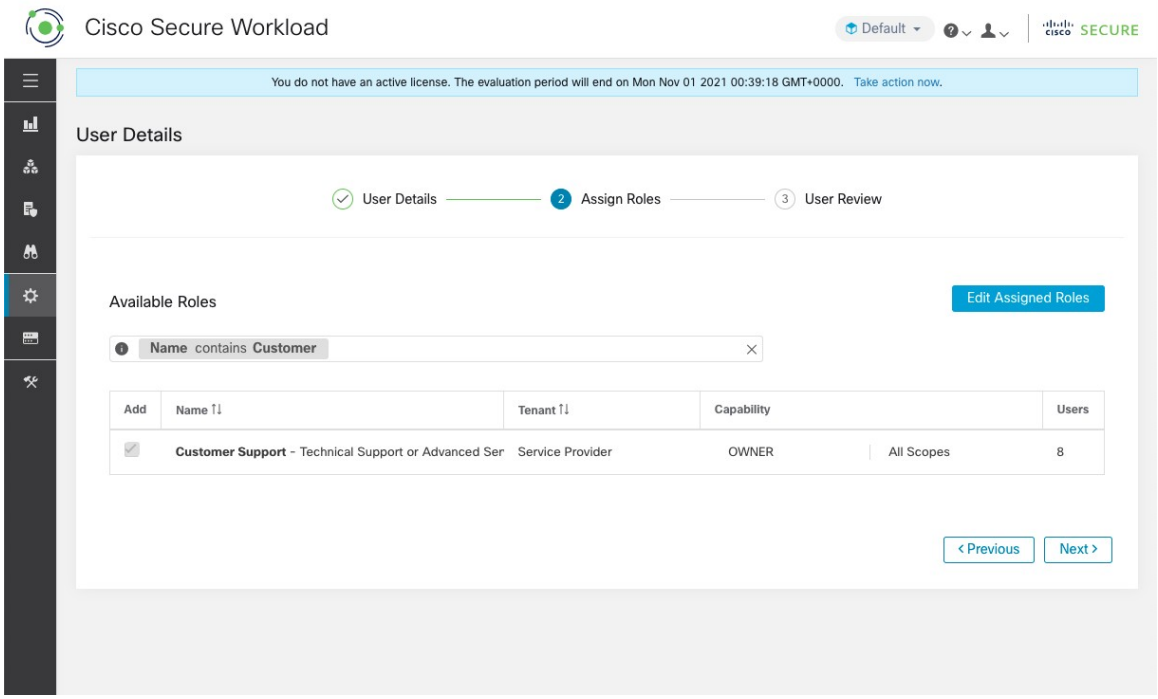
Figure 583: Rôles d'utilisateurs attribués



- Sélectionnez les rôles attribués, cliquez sur **Edit Assigned Roles** (Modifier les rôles attribués), puis cliquez sur l'icône **Remove** (Supprimer).

- Vous pouvez filtrer les rôles d'utilisateur à l'aide du **nom** ou du **détenteur**.

Figure 584: Filtrer les rôles d'utilisateur



Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Sous **User Review** (Révision de l'utilisateur), vérifiez les détails de l'utilisateur et les rôles qui lui sont attribués. Cliquez sur **Create** (créer).

Si l'authentification externe est activée, les détails de l'authentification s'affichent.

Note Une fois l'utilisateur ajouté à Cisco Secure Workload, un courriel d'activation est envoyé à l'ID de courriel enregistré pour configurer le mot de passe.

Modifier les détails ou le rôle d'un utilisateur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour modifier des utilisateurs dans Cisco Secure Workload.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Le cas échéant, sélectionnez la portée racine appropriée dans l'en-tête de page.

Étape 2 Dans le volet de navigation, choisissez **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 3 Pour le compte d'utilisateur requis, sous **Actions**, cliquez sur **Edit** Modifier).
La page **User Details** (des détails de l'utilisateur) s'affiche.

Étape 4 Modifiez les détails suivants.

a) Mettez à jour les champs suivants sous **User Details** (Détails sur l'utilisateur) .

Table 64: Description des champs des détails de l'utilisateur

Champ	Description
Email	Mettez à jour l'identifiant de courriel de l'utilisateur.
Prénom	Mettez à jour le prénom de l'utilisateur.
Nom	Mettez à jour le nom de famille de l'utilisateur.
Scope	La portée racine qui est affectée à l'utilisateur pour l'architecture multidétenteurs. (Disponible pour les administrateurs du site)

b) Cliquez sur **Next** (suivant).

c) Sous **Assign Roles** (Affecter des rôles), ajoutez ou supprimez des rôles attribués à l'utilisateur.

- Cliquez sur **Add rôles** (Ajouter des rôles) pour attribuer de nouveaux rôles, puis cochez la case **Add** (ajouter).
- Sélectionnez les rôles attribués, cliquez sur **Edit Assigned Roles** (Modifier les rôles attribués), puis cliquez sur l'icône **Remove** (Supprimer).

d) Cliquez sur **Next** (suivant).

e) Sous **User Review** (Révision de l'utilisateur), vérifiez les détails de l'utilisateur et les rôles qui lui sont attribués. Cliquez sur **Update** (Mettre à jour) pour mettre à jour le compte d'utilisateur.

Si l'authentification externe est activée, les détails de l'authentification s'affichent.

Désactivation d'un compte d'utilisateur

Note Pour maintenir la cohérence des vérifications des journaux des modifications, les utilisateurs ne peuvent qu'être désactivés, ils ne sont pas supprimés de la base de données.

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour ce faire.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 2 Le cas échéant, sélectionnez la portée racine appropriée dans le coin supérieur droit de la page.

Étape 3 À la ligne du compte que vous souhaitez désactiver, cliquez sur le bouton **Deactivate** (Désactiver) dans la colonne de droite.

Pour afficher les utilisateurs désactivés, utilisez le bouton à bascule **Hide Deleted Users** (Masquer les utilisateurs supprimés).

Réactivation d'un compte d'utilisateur

Si un utilisateur a été désactivé, vous pouvez le réactiver.

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour ce faire.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 2 Le cas échéant, sélectionnez la portée racine appropriée dans le coin supérieur droit de la page.

Étape 3 Activez ou désactivez l'option **Hide Deleted Users** (Masquer les utilisateurs supprimés) pour afficher tous les utilisateurs, y compris les utilisateurs désactivés.

Étape 4 Pour le compte désactivé requis, cliquez sur **Restore** (Restaurer) dans la colonne de droite pour réactiver le compte.

Importer une clé publique SSH

Pour activer l'accès SSH en tant qu'utilisateur **ta_guest** via l'une des adresses IP de collecteur, la clé publique SSH peut être importée pour chaque utilisateur. Ce menu est uniquement disponible pour les **administrateurs de site** et les utilisateurs avec la capacité `SCOPE_OWNER` (Propriétaire de portée) sur la portée racine. La clé publique SSH expire automatiquement dans 7 jours.

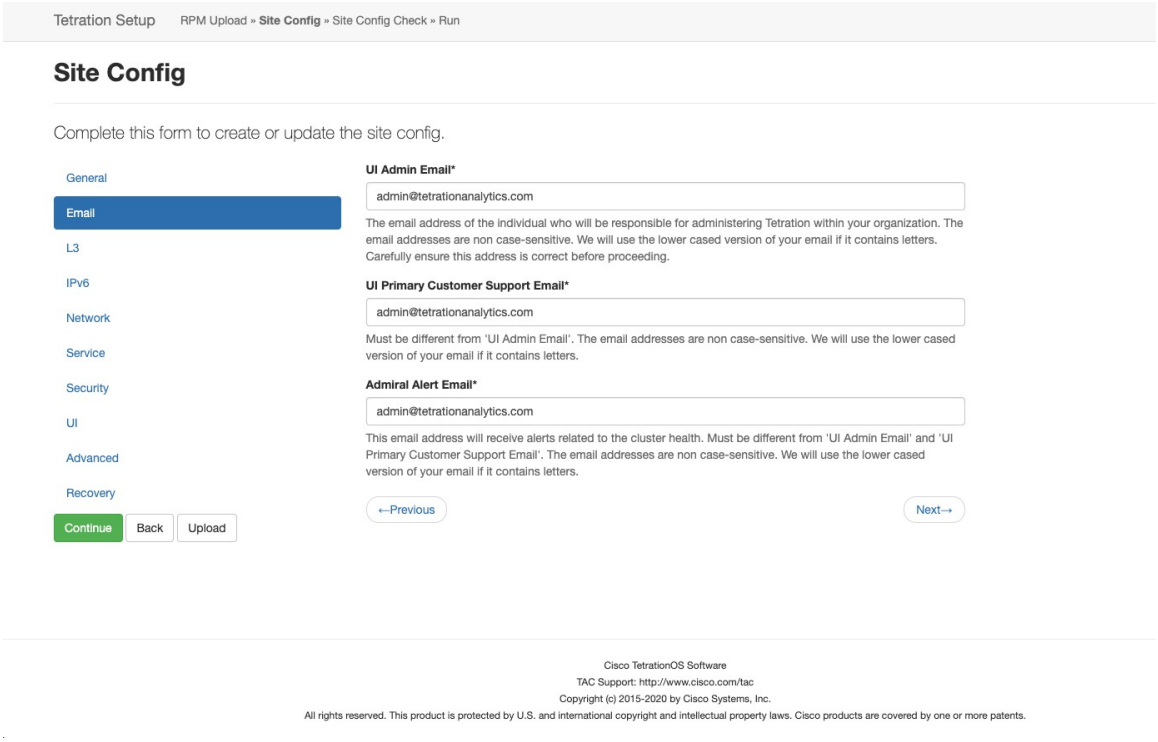
Configuration du site dans l'installation de Cisco Secure Workload

Cette section explique comment les **administrateurs de site** peuvent configurer un site pendant le processus de configuration Cisco Secure Workload.

Champ	Description
Courriel de l'administrateur 'interface utilisateur	L'adresse courriel de la personne qui sera responsable de l'administration de Cisco Secure Workload au sein de votre organisation.
Adresse courriel principale du service d'assistance à la clientèle de l'interface utilisateur	L'adresse courriel du service d'assistance principal. Doit être différent du courriel de l'administrateur de l'interface utilisateur.
Courriel d'alerte Admiral	Cette adresse courriel reçoit les alertes relatives à l'intégrité de la grappe. Doit être différent de l'adresse courriel de l'administrateur de l'interface utilisateur et de l'adresse courriel du service d'assistance à la clientèle principal de l'interface utilisateur.

Les adresses courriel ne sont pas sensibles à la casse. Nous utilisons la version en minuscules de votre courriel s'il contient des lettres.

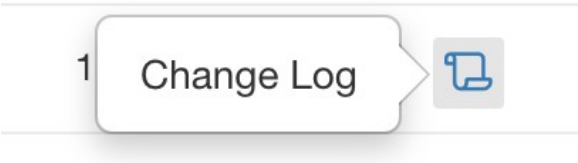
Figure 585: Configurer les courriels d'alerte de l'administrateur de l'interface utilisateur, du service d'assistance à la clientèle principal et de l'administrateur Admiral



Journal des modifications : Utilisateurs

Les **administrateurs de site** et les utilisateurs qui ont la capacité `SCOPE_OWNER` (PROPRIÉTAIRE_PORTÉE) sur la portée racine peuvent afficher les journaux des modifications pour chaque utilisateur en cliquant sur l'icône dans la colonne **Actions**, comme l'illustre la figure suivante.

Figure 586: Journal des modifications



Pour en savoir plus sur le **journal des modifications**, consultez le Journal des modifications. Les propriétaires de la portée racine peuvent uniquement afficher les entrées du journal des modifications pour les entités appartenant à leur portée.

CHAPITRE 18

Cisco Secure Workload OpenAPI

OpenAPI fournit une API REST pour les fonctionnalités Cisco Secure Workload.

Authentification OpenAPI

OpenAPI utilise un schéma d'authentification basé sur un condensé. Le flux de travail est le suivant :

1. Connectez-vous au tableau de bord de l'interface utilisateur Cisco Secure Workload.
2. Générer une clé API et un code secret API avec les capacités souhaitées.
3. Utilisez le SDK API Cisco Secure Workload pour envoyer des requêtes REST au format JSON.
4. Pour utiliser le SDK Python, installez-le à l'aide de la `commande pip install tetpyclient`.
5. Une fois le SDK Python installé, voici un code standard pour l'instanciation de RestClient :

```
from tetpyclient import RestClient

API_ENDPOINT="https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"

# ``verify`` is an optional param to disable SSL server authentication.
# By default, cluster dashboard IP uses self signed cert after
# deployment. Hence, ``verify=False`` might be used to disable server
# authentication in SSL for API clients. If users upload their own
# certificate to cluster (from ``Platform > SSL Certificate``)
# which is signed by their enterprise CA, then server side authentication
# should be enabled; in such scenarios, in the code below, verify=False
# should be replaced with verify="path-to-CA-file"
# credentials.json looks like:
# {
#   "api_key": "<hex string>",
#   "api_secret": "<hex string>"
# }

restclient = RestClient(API_ENDPOINT,
                credentials_file='<path_to_credentials_file>/credentials.json',
                verify=False)
# followed by API calls, for example API to retrieve list of agents.
# API can be passed /openapi/v1/sensors or just /sensors.
resp = restclient.get('/sensors')
```

Générer une clé API et un code secret

Procedure

Étape 1 Dans le coin supérieur droit de l'interface utilisateur Cisco Secure Workload, cliquez sur le compte connecté et sélectionnez **API Keys** (Clés API).

Étape 2 Cliquez sur **Create API Key** (créer une clé API).

Étape 3 (Facultatif) Saisissez une description pour la clé API.

Étape 4 Sélectionnez les fonctionnalités requises pour la clé et le code secret.

Sélectionnez l'ensemble limité de fonctionnalités destinées à l'utilisation de la paire clé API + code secret.

Note La disponibilité des fonctionnalités de l'API varie selon le rôle de l'utilisateur.

Table 65: Fonctionnalités de l'API

Capacité	Description
`sensor_management`	Pour configurer et surveiller l'état des agents logiciels
`software_download`	Pour télécharger des progiciels pour des agents ou des appliances virtuelles
`flow_inventory_query`	Pour interroger les flux et les articles de l'inventaire de la grappe Cisco Secure Workload
`user_role_scope_management`	Pour lire, ajouter, modifier ou supprimer des utilisateurs, des rôles et des portées
`user_data_upload`	Pour permettre aux utilisateurs de téléverser des données pour annoter les flux et les éléments d'inventaire ou de téléverser des condensés (hachages) de fichiers corrects ou non valides
`app_policy_management`	Pour gérer les espaces de travail (applications) et appliquer les politiques
`external_integration`	Pour permettre l'intégration avec des systèmes externes tels que vCenter et Kubernetes

Table 66: Capacités d'API pour les administrateurs de site

Capacité	Description
`appliance_management`	Pour gérer les appareils Cisco Secure Workload
`appliance_monitoring`	Pour surveiller les paramètres et la configuration des appareils Cisco Secure Workload (en lecture seule)

Étape 5 Cliquez sur **Create** (créer).

La clé API et le code secret sont générés, puis doivent être copiés dans un fichier et enregistrés dans un emplacement sûr. Sinon, vous pouvez télécharger le fichier JSON avec la clé et le code secret.

Note Si les options External Auth with LDAP (Authentification externe avec LDAP) et LDAP Authorization (Autorisation LDAP) sont activées, l'accès à OpenAPI à l'aide des clés API s'arrête parce que les rôles Cisco Secure Workload dérivés des groupes LDAP MemberOf (Membre de LDAP) sont réévalués après la fin de la session utilisateur. Par conséquent, pour assurer un accès OpenAPI ininterrompu, il est recommandé à tout utilisateur disposant de clés API d'activer l'option **Use Local Authentication** (Utiliser l'authentification locale) dans le flux Edit User Details (modifier les détails de l'utilisateur) de ce dernier.

Espaces de travail et politiques de sécurité

Les pages suivantes décrivent les points terminaux OpenAPI pour gérer la Gérer le cycle de vie des politiques dans Cisco Secure Workload.

Espaces de travail

Les espaces de travail (anciennement « espaces de travail d'applications » ou « applications ») sont les conteneurs qui permettent de définir, d'analyser et d'appliquer les politiques pour les charges de travail dans une portée spécifique. Pour en savoir plus sur leur fonctionnement, consultez la documentation sur les Utiliser des espaces de travail pour gérer les politiques. Cet ensemble d'API nécessite la capacité `app_policy_management` associée à la clé API.

Objet espace de travail

L'objet JSON d'espace de travail (« application ») est renvoyé sous forme d'objet unique ou de tableau d'objets selon le point terminal d'API. Les attributs de l'objet sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Un identifiant unique pour l'espace de travail.
name	chaîne	Nom spécifié par l'utilisateur de l'espace de travail.
description	chaîne	Description de l'espace de travail précisée par l'utilisateur.
app_scope_id	chaîne	ID de la portée auquel l'espace de travail est associé.
auteur	chaîne	Prénom et nom de famille de l'utilisateur qui a créé l'espace de travail.
principal	booléen	Indique si l'espace de travail est principal pour sa portée.

Attribut	Type	Description
alternate_query_mode	booléen	Indique si le « mode dynamique » est utilisé pour l'espace de travail. En mode dynamique, une exécution de découverte automatique des politiques crée une ou plusieurs requêtes admissibles pour chaque grappe. La valeur par défaut est « vrai ».
created_at	nombre entier	Horodatage Unix de la création de l'espace de travail.
latest_adm_version	nombre entier	La dernière version adm (v*) de l'espace de travail.
analysis_enabled	booléen	Indique si l'analyse est activée sur l'espace de travail.
analyzed_version	nombre entier	La version p* analysée de l'espace de travail.
enforcement_enabled	booléen	Indique si l'application est activée pour l'espace de travail.
enforced_version	nombre entier	La version p* appliquée de l'espace de travail.

Répertorier les applications

Ce point terminal renverra un tableau d'espaces de travail (« applications »).

```
GET /openapi/v1/applications
```

Table 67: Paramètres

Nom	Type	Description
app_scope_id	chaîne	Fait correspondre des espaces de travail associés à une portée d'application spécifique.
exact_name	chaîne	Fait correspondre les espaces de travail avec exactement la valeur fournie.

Objet de réponse : renvoie un tableau des objets espace de travail.

Exemple de code Python

```
restclient.get('/applications')
```

Récupérer un seul espace de travail

Ce point terminal renverra l'espace de travail demandé (« application ») en tant qu'objet JSON unique.

```
GET /openapi/v1/applications/{application_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Objet de réponse : renvoie l'objet espace de travail pour l'ID spécifié.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
restclient.get('/applications/%s' % application_id)
```

Créer un espace de travail

Ce point terminal crée un espace de travail (« application »). Il est possible de définir des politiques en publiant un corps JSON contenant les définitions de la grappe et des politiques.

Note S'il existe un espace de travail principal pour la même portée et que de nouvelles politiques sont fournies, les politiques seront ajoutées en tant que nouvelle version à l'espace de travail existant.

```
POST /openapi/v1/applications
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
app_scope_id	chaîne	L'ID de la portée à affecter à l'espace de travail.
name	chaîne	(Facultatif) Un nom pour l'espace de travail.
description	chaîne	(Facultatif) La description mise à jour de l'espace de travail.
alternate_query_mode	booléen	(Facultatif) Indique si le « mode dynamique » est utilisé pour l'espace de travail. En mode dynamique, une exécution de découverte automatique des politiques crée une ou plusieurs requêtes admissibles pour chaque grappe. La valeur par défaut est « vrai ».
strict_validation	booléen	(Facultatif) Renvoie une erreur s'il y a des clés ou des attributs inconnus dans les données téléversées. Utile pour détecter les clés mal épelées. La valeur par défaut est faux.

Nom	Type	Description
principal	chaîne	(Facultatif) Définissez sur « vrai » si cet espace de travail doit être principal pour la portée associée. **La valeur par défaut est « vrai »**

Des paramètres facultatifs supplémentaires peuvent être inclus pour décrire les politiques à créer dans l'espace de travail.

Note Le schéma correspond à celui renvoyé lors de l'exportation par l'interface utilisateur et le point terminal **Details**.

Nom	Type	Description
grappes	tableau de grappes	Groupes de nœuds à utiliser pour définir des politiques
inventory_filters	tableau de filtres d'inventaire	Ressources du centre de données
absolute_policies	tableau de politiques	Ordonnancement des politiques à créer avec le rang absolu.
default_policies	tableau de politiques	Ordonnancement des politiques à créer avec le rang par défaut .
catch_all_action	chaîne	« AUTORISER » ou « REFUSER »

Attributs de l'objet de la grappe :

Nom	Type	Description
ID	chaîne	Identifiant unique à utiliser avec les politiques.
name	chaîne	Nom affiché de la grappe.
description	chaîne	Description de la grappe.
nœuds	tableau de nœuds	Les nœuds ou les points terminaux qui font partie de la grappe.
consistent_uuid	chaîne	Doit être unique à un espace de travail donné. Après une exécution de découverte automatique des politiques, les grappes similaires/identiques de la prochaine version maintiendront l'attribut consistent_uuid.

Attributs de l'objet nœud :

Nom	Type	Description
ip	chaîne	IP ou sous-réseau du nœud Par exemple 10.0.0.0/8 ou 1.2.3.4
name	chaîne	Nom affiché du nœud.

Attributs de l'objet filtre d'inventaire :

Nom	Type	Description
ID	chaîne	Identifiant unique à utiliser avec les politiques.
name	chaîne	Nom affiché de la grappe.
query	objet	Représentation objet JSON d'une requête de filtre d'inventaire.

Attributs de l'objet politiques :

Nom	Type	Description
consumer_filter_id	chaîne	ID d'une grappe, d'un filtre d'inventaire d'utilisateurs ou de la portée de l'application.
provider_filter_id	chaîne	ID d'une grappe, d'un filtre d'inventaire d'utilisateurs ou de la portée de l'application.
action	chaîne	« AUTORISER » ou « REFUSER »
l4_params	tableau de l4params	Liste des ports et des protocoles autorisés.

Attributs de l'objet L4Params :

Nom	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	tableau	Plage de ports inclusive. Par exemple, [80, 80] ou [5000, 6000].
approved	booléen	(Facultatif) Indique si la politique est approuvée. La valeur par défaut est False.

Objet de réponse : renvoie l'objet espace de travail nouvellement créé.

Exemple de code Python

```
name = 'test'
scope_id = '5ce480cc497d4f1b4b9a9e8d'
filter_id = '5ce480cd497d4f1b4b9a9ea4'
application = {
    'app_scope_id': scope_id,
    'name': name,
    'absolute_policies': [
```

```
            {
        # consumer/provider filter IDs can be ID of a cluster identified during automatic
policy discovery (formerly known as ADM),
        # user inventory filter or app scope.
                'provider_filter_id': filter_id,
                'consumer_filter_id': filter_id,
                'action': 'ALLOW',
        # ALLOW policy for TCP on port 80.
                'l4_params': [
                    {
                        'proto': 6, # TCP
                        'port': [80, 80],  # port range
                    }
                ],
            }
        ],
        'catch_all_action': 'ALLOW'
    }
    restclient.post('/applications', json_body=json.dumps(application))
```

Importer une nouvelle version

Importe les politiques et crée une nouvelle version v* pour l'espace de travail (« application »).

`POST /openapi/v1/applications/{application_id}/import`

Les paramètres sont les mêmes que pour le point terminal de création d'espace de travail.

Objet de réponse : renvoie l'objet de l'espace de travail.

Valider un ensemble de politiques

Valide un ensemble de politiques sans créer de nouvelle version.

`POST /openapi/v1/applications/validate_policies`

Un *app_scope_id* est obligatoire. Les autres paramètres sont identiques à ceux du point terminal de création d'espace de travail.

Objet de réponse :

Attribut	Type	Description
valide	booléen	Indique si les politiques sont valides
erreurs	tableau	Si non valide, détails sur les erreurs

Supprimer un espace de travail

Supprime un espace de travail (une« application »).

`DELETE /openapi/v1/applications/{application_id}`

La mise en application doit être désactivée sur l'espace de travail avant de pouvoir le supprimer.

Si l'espace de travail, ou ses grappes, est utilisé par d'autres applications (par une relation de service fourni), ce point terminal renverra le message `422 Unprocessable Entity` (422 Entité non traitable). L'objet Erreur renvoyé contiendra un attribut `détails` avec le nombre d'objets dépendants ainsi que les ID des 10 premiers de chaque type. Ces renseignements peuvent être utilisés pour localiser et supprimer les dépendances bloquantes.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Objet de réponse : aucun

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
restclient.delete('/applications/%s' % application_id)
```

Mettre à jour un espace de travail

Ce point terminal met à jour un espace de travail existant (« application »).

```
PUT /openapi/v1/applications/{application_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
name	chaîne	(Facultatif) Le nom mis à jour de l'espace de travail.
descrip	chaîne	(Facultatif) La description mise à jour de l'espace de travail.
principal	chaîne	(Facultatif) Définissez à la valeur « vrai » pour en faire l'espace de travail principal. Définissez la valeur « faux » pour rendre l'espace de travail secondaire.

Objet de réponse : l'objet d'espace de travail mis à jour pour l'ID spécifié.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
req_payload = {
      'name': 'Updated Name',
      'description': 'Updated Description',
      'primary': 'true'
}
resp = restclient.put('/applications/%s' % application_id,
                      json_body=json.dumps(req_payload))
```

Récupérer les détails de l'espace de travail

Ce point terminal renvoie un fichier JSON d'exportation complet pour l'espace de travail. Il comprend les définitions de politique et de grappe.

```
GET /openapi/v1/applications/{application_id}/details
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
version	chaîne	(Facultatif) Une version sous la forme « v10 » ou « p10 », par défaut, « latest » (dernière).

Objet de réponse : renvoie les grappes et les politiques dans la version d'espace de travail donnée.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
# For v* version v10 and for p* version p10
version = 'v10'
resp = restclient.get('/applications/%s/details?version=%s' % (application_id, version))
```

Répertorier les versions d'espace de travail

Ce point terminal renverra une liste de toutes les versions pour un espace de travail donné.

```
GET /openapi/v1/applications/{application_id}/versions
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
created_before	nombre entier	(Facultatif) Pour la pagination, définissez la valeur « created_at » de la dernière version de la réponse précédente.
limit	nombre entier	(Facultatif) Nombre maximal de résultats à renvoyer, la valeur par défaut est 50.

Objet de réponse : un tableau d'objets ayant les attributs suivants :

Attribut	Type	Description
version	chaîne	Une version sous la forme « v10 » ou « p10 ».

Attribut	Type	Description
created_at	nombre entier	Horodatage Unix de la création de l'espace de travail.
description	chaîne	Description fournie par l'utilisateur
name	chaîne	Nom d'affichage

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
created_before = 1612325705
limit = 10
resp = restclient.get('/applications/%s/versions?created_before=%s&limit=%s' %
                      (application_id, created_before, limit))
```

Supprimer la version de l'espace de travail

Ce point terminal supprimera la version donnée, y compris les grappes et les politiques. Les versions appliquées ou analysées ne peuvent pas être supprimées. Si des membres sont référencés par un autre espace de travail, par le biais d'une politique externe, la réponse renvoie une erreur avec une liste des références.

```
DELETE /openapi/v1/applications/{application_id}/versions/{version}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
version	chaîne	Une version sous la forme « v10 » ou « p10 ».

Objet de réponse : aucun

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
version = 'v10'
resp = restclient.delete('/applications/%s/versions/%s' %
                         (application_id, version))
```

Comparer les versions de l'espace de travail

Ce point terminal calcule la différence entre les versions de l'espace de travail fournies. Il retourne les politiques ajoutées, supprimées et éventuellement inchangées. Les modifications apportées à la grappe sont incluses si la grappe est présente dans les deux versions, définie par un _uuid cohérent correspondant, et que la requête a été modifiée.

```
GET /openapi/v1/applications/{application_id}/version_diff
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
base_version	chaîne	Version complète, par exemple « v10 » ou « p10 ».
draft_version	chaîne	Version complète, par exemple « v10 » ou « p10 ».
include_unchanged	booléen	La valeur par défaut est False. Renvoie les politiques inchangées dans la réponse.

Objet de réponse : renvoie un objet avec les attributs suivants :

Attribut	Type	Description
grappes	tableau	Les grappes qui ont été modifiées entre les versions.
politiques	tableau	Les politiques qui ont été modifiées entre les versions.

Analyser les dernières politiques

Activez l'analyse du dernier ensemble de règles dans l'espace de travail.

```
POST /openapi/v1/applications/{application_id}/enable_analysis
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Paramètres : le corps facultatif de la requête JSON contient les clés suivantes :

Nom	Type	Description
action_note	chaîne	(Facultatif) Raison de l'action de publication des politiques.
name	chaîne	(Facultatif) Nom dans la version de politique publiée.
description	chaîne	(facultatif) une description dans la version de politique publiée.

Objet de réponse : renvoie un objet avec les attributs suivants :

Attribut	Type	Description
data_set	objet	Représentation sous forme d'objet JSON de l'ensemble de données.
analyzed_policy_version	nombre entier	La version p* analysée de l'espace de travail.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
req_payload = {
  'action_note': 'Policy analysis',
  'name': 'Test run 1',
  'description': 'New workloads added.'
}
resp = restclient.post('/applications/%s/enable_analysis' % application_id,
                       json_body=json.dumps(req_payload))
```

Désactiver l'analyse des politiques sur un seul espace de travail

Désactiver l'analyse des politiques sur l'espace de travail.

```
POST /openapi/v1/applications/{application_id}/disable_analysis
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Objet de réponse : renvoie un objet avec les attributs suivants :

Attribut	Type	Description
data_set	objet	Représentation sous forme d'objet JSON de l'ensemble de données.
analyzed_policy_version	nombre entier	Dernière version p* analysée de l'espace de travail.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
resp = restclient.post('/applications/%s/disable_analysis' % application_id)
```

Appliquer un espace de travail unique

Activez l'application du dernier ensemble de politiques dans l'espace de travail.

```
POST /openapi/v1/applications/{application_id}/enable_enforce
```

Warning De nouvelles règles de pare-feu d'hôte seront insérées et toutes les règles existantes seront supprimées sur les hôtes concernés.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
version	chaîne	(Facultatif) La version de la politique à appliquer.

Si aucune version n'est fournie, les dernières politiques de l'espace de travail seront appliquées. « versions » doit être de manière préférentielle sous la forme « p* »; si seul un entier est fourni, la version « p* » correspondante sera appliquée.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
heure d'origine	chaîne	Identifiant unique du dernier profil d'application de la loi.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
req_payload = {
  'version': 'p10'
}
resp = restclient.post('/applications/%s/enable_enforce' % application_id,
                       json_body=json.dumps(req_payload))
```

Désactiver l'application pour un seul espace de travail

Désactivez l'application sur l'espace de travail.

```
POST /openapi/v1/applications/{application_id}/disable_enforce
```

Warning De nouvelles règles de pare-feu d'hôte seront insérées et toutes les règles existantes seront supprimées sur les hôtes concernés.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
heure d'origine	chaîne	Identifiant unique du dernier profil d'application de la loi.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
resp = restclient.post('/applications/%s/disable_enforce' %
                       application_id)
```

Initier la découverte automatique des politiques

Détectez automatiquement les politiques pour l'espace de travail. (anciennement dénommé « soumission d'une exécution ADM »).

```
POST /openapi/v1/applications/{application_id}/submit_run
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
start_time	chaîne	Heure de début de l'intervalle d'entrée pour une exécution de découverte automatique de politiques.
end_time	chaîne	Heure de fin de l'intervalle d'entrée pour une exécution de découverte automatique de politique.
clustering_granularity	chaîne	(Facultatif) Granularité de la grappe permet à l'utilisateur de contrôler la taille des grappes générées par la découverte automatique des politiques. Valeurs attendues : VERY_FINE, FINE, MEDUM, COARSE ou VERY_COARSE

Nom	Type	Description
port_generalization	chaîne	(Facultatif) Généralisation des ports contrôle le niveau de signification statistique requis lors de la généralisation de port. Valeurs attendues : DISABLED, CONSERVATIVE, MODERATE, AGRESSIVE ou VERY_AGGRESSIVE
policy_compression	chaîne	(Facultatif) Compression des politiques lorsqu'elle est activée, les politiques qui sont suffisamment fréquentes, c'est-à-dire qui utilisent le même port fournisseur, parmi les grappes générées à l'intérieur d'un espace de travail peuvent être "factorisées" vers le parent, c'est-à-dire remplacées par une ou plusieurs politiques applicables à l'ensemble de la portée parente. Valeurs attendues : DISABLED, CONSERVATIVE, MODERATE, AGRESSIVE ou VERY_AGGRESSIVE
auto_accept_policy_connectors	booléen	(facultatif) Connecteurs de politiques d'acceptation automatique de politique Toutes les demandes de politique sortantes créées lors de la découverte automatique des politiques sont automatiquement acceptées.
enable_exclusion_filter	booléen	(Facultatif) L'option Activer le filtre d'exclusion offre la possibilité d'ignorer toutes les conversations correspondant à l'un des filtres d'exclusion définis par l'utilisateur (le cas échéant). Pour en savoir plus, consultez Filtres d'exclusion.
enable_default_exclusion_filter	booléen	(Facultatif) L'option Activer le filtre d'exclusion par défaut offre la possibilité d'ignorer toutes les conversations correspondant à l'un des filtres d'exclusion par défaut (le cas échéant). Consultez la section Filtres d'exclusion par défaut pour en savoir plus.

Nom	Type	Description
enable_service_discovery	booléen	(Facultatif) Lorsque l'option Activer la découverte de service sur l'agent (Activer la découverte de services sur l'agent) est définie, des informations éphémères de plage de ports sont fournies sur les services présents sur le nœud de l'agent. Des politiques sont ensuite générées en fonction des informations de plage de ports signalées.
carry_over_policies	booléen	(facultatif) Lorsque Reporter des politiques approuvées (report des politiques approuvées) est défini, toutes les politiques marquées comme approuvées par l'utilisateur dans l'interface utilisateur ou OpenAPI seront conservées.
skip_clustering	booléen	(Facultatif) Lorsque l'option Ignorer la mise en grappe et générer uniquement les politiques(Ignorer la mise en grappe) est définie, aucune nouvelle grappe n'est générée, et les politiques sont générées à partir de toutes les grappes approuvées existantes ou des filtres d'inventaire et impliquent toutes les charges de travail de la portée.
deep_policy_generation	booléen	(Facultatif) Vous pouvez générer des politiques pour une branche de l'arborescence de la portée plutôt que pour une seule portée. Pour en savoir plus, consultez Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée, on page 453 et les sous-sections.

Nom	Type	Description
use_default_config	booléen	(Facultatif) Lorsque cette option est définie, la découverte automatique des politiques utilise la configuration de la découverte des politiques par défaut au lieu de la configuration d'exécution précédente. Pour en savoir plus, consultez Configuration de la découverte de politiques par défaut.

Note Les valeurs par défaut des paramètres facultatifs non spécifiés seront issues de la configuration précédente de la découverte automatique des politiques si cette dernière a été effectuée plus tôt dans l'espace de travail, sinon les valeurs par défaut seront tirées de la configuration de découverte des politiques par défaut.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
message	chaîne	Message concernant la réussite ou l'échec de l'exécution de la découverte automatique des politiques.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
req_payload = {
      'start_time': '2020-09-17T10:00:00-0700',
      'end_time': '2020-09-17T11:00:00-0700',
      # Optional Parameters.
      'clustering_granularity': 'FINE',
      'port_generalization': 'AGGRESSIVE',
      'policy_compression': 'AGGRESSIVE',
      'auto_accept_policy_connectors': False,
      'enable_exclusion_filter': True,
      'enable_default_exclusion_filter': True,
      'enable_service_discovery': True,
      'carry_over_policies': True,
      'skip_clustering': False,
      'deep_policy_generation': True,
      'use_default_config': False
}
resp = restclient.post('/applications/%s/submit_run' % application_id,
                       json_body=json.dumps(req_payload))
```

Obtenir l'état d'une exécution de découverte de politiques

Recherchez l'état d'une exécution de découverte automatique de politique dans l'espace de travail.

```
GET /openapi/v1/applications/{application_id}/adm_run_status
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
état	chaîne	État de l'exécution de la découverte automatique des politiques. Valeurs : PENDING (EN COURS), COMPLETE (TERMINÉ) ou FAILED (ERREUR)

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
resp = restclient.get('/applications/%s/adm_run_status' % application_id)
```

Politiques

Cet ensemble d'API peut être utilisé pour gérer l'ajout, la modification ou la suppression de politiques. Le paramètre de `version` est requis pour les actions Collecte de toutes les créations et mises à jour. Ces renseignements nécessitent la capacité `user_role_scope_management` associée à la clé API.

Objet politique

Les attributs de l'objet de politique sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique de la politique.
application_id	chaîne	ID de l'espace de travail auquel la politique appartient.
consumer_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe, tout filtre défini par l'utilisateur ou toute portée peut être utilisé comme consommateur d'une politique.
provider_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe, tout filtre défini par l'utilisateur ou toute portée peut être utilisé comme fournisseur d'une politique.
version	chaîne	Indique la version de l'espace de travail auquel la politique appartient.

Attribut	Type	Description
rank	chaîne	Rang de politique, valeurs possibles : DEFAULT (PAR DÉFAUT), ABSOLUTE (ABSOLUE) ou CATCHALL COLLECTRICE).
policy_action	chaîne	Les valeurs possibles peuvent être ALLOW (AUTORISER) ou DENY (REFUSER). Indique si le trafic doit être autorisé ou abandonné pour un port de service ou un protocole entre le consommateur et le fournisseur de service.
priority	nombre entier	Utilisé pour trier les politiques.
l4_params	tableau de l4params	Liste des ports et des protocoles autorisés.

Attributs de l'objet L4Params :

Nom	Type	Description
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	tableau	Gamme de ports inclusive. ex., [80, 80] ou [5000, 6000].
description	chaîne	Chaîne courte concernant ce protocole et ce port.
approved	booléen	Si la politique a été approuvée par l'utilisateur.

Obtenir des politiques

Ce point terminal renvoie une liste des politiques dans un espace de travail particulier. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/policies
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
version	chaîne	Indique la version de l'espace de travail à partir duquel obtenir les politiques.

Nom	Type	Description
consumer_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID du filtre du consommateur.
provider_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID du filtre du consommateur.

Les ID de politiques peuvent changer d'une version à l'autre. Pour obtenir la liste des politiques d'une version publiée, le numéro de version doit être précédé d'un « p ». Par exemple, pour récupérer toutes les politiques dans la version publiée 3, nous pouvons effectuer une requête comme :

```
GET /openapi/v1/applications/{application_id}/policies?version=p3
```

Renvoie un objet de toutes les politiques de cet espace de travail particulier, comme indiqué ci-dessous

```
{
  absolute_policies: [ ... ],
  default_policies: [ ... ],
  catch_all_action:
}
```

Exemple de code Python

```
application_id = '5f88c996755f023f3bafe163'
restclient.get('/applications/%s/policies' % application_id, params={'version': '1'})
```

Obtenir les politiques par défaut

Ce point terminal renvoie une liste des politiques par défaut pour un espace de travail donné. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/default_policies
```

Paramètres :

Nom	Type	Description
ID	chaîne	Identifiant unique de la politique.
version	chaîne	Indique la version de l'espace de travail pour lequel obtenir les politiques.
limit	nombre entier	Limite le nombre de politiques par demande.
offset	nombre entier	(Facultatif) Nombre de décalage reçu de la réponse précédente, doit toujours être utilisé avec `limite`.
consumer_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID du filtre du consommateur.

Nom	Type	Description
provider_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID de filtre du fournisseur.

Renvoie la liste des politiques par défaut dans la version fournie de cet espace de travail. La réponse contient le nombre de politiques demandé et un `décalage`, pour obtenir le prochain ensemble de politiques, utilisez ce `décalage` dans les demandes suivantes. L'absence de `décalage` dans la réponse indique que toutes les politiques sont déjà extraites.

Exemple de code Python

```
  application_id = '5f88c996755f023f3bafe163'
  restclient.get('/applications/%s/default_policies' % application_id, params={'version':
'1', 'limit': 3, 'offset': 3})
```

Exemple de réponse

```
    {
      "results": [
      PolicyObject4,
      PolicyObject5,
      PolicyObject6
      ],
      "offset": 6
    }
```

Obtenir les politiques absolues

Ce point terminal renvoie une liste des politiques absolues dans un espace de travail donné. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/absolute_policies
```

Paramètres :

Nom	Type	Description
version	chaîne	Indique la version de l'espace de travail à partir duquel obtenir les politiques.
limit	nombre entier	Limite le nombre de politiques par demande.
offset	nombre entier	(Facultatif) Nombre de décalage reçu de la réponse précédente, doit toujours être utilisé avec `limite`.
consumer_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID du filtre du consommateur.

Nom	Type	Description
provider_filter_id	chaîne	(Facultatif) Filtre la sortie en fonction de l'ID de filtre du fournisseur.

Renvoie la liste des politiques absolues dans la version fournie de cet espace de travail. La réponse contient le nombre de politiques demandé et un `décalage`, pour obtenir le prochain ensemble de politiques, utilisez ce `décalage` dans les demandes suivantes. L'absence de `décalage` dans la réponse indique que toutes les politiques sont déjà extraites.

Exemple de code Python

```
  application_id = '5f88c996755f023f3bafe163'
  restclient.get('/applications/%s/absolute_policies' % application_id, params={'version':
'1', 'limit': 3})
```

Exemple de réponse

```
    {
      "results": [
      PolicyObject1,
      PolicyObject2,
      PolicyObject3
      ],
      "offset": 3
    }
```

Obtenir les politiques Catch All (collectrices)

Ce point terminal renvoie une politique Catch All (collectrice) pour un espace de travail donné. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/catch_all
```

Paramètres :

Nom	Type	Description
version	chaîne	Indique la version de l'espace de travail à partir duquel obtenir les politiques.

Renvoie un objet de politique unique représentant la politique collectrice d'une version donnée de l'espace de travail.

Exemple de code Python

```
  application_id = '5f88c996755f023f3bafe163'
  restclient.get('/applications/%s/catch_all' % application_id, params={'version': '1'})
```

Obtenir une politique spécifique

Ce point terminal renvoie une instance d'une politique.

```
GET /openapi/v1/policies/{policy_id}
```

Renvoie l'objet de politique associé à l'ID spécifié.

Exemple de code Python

```
policy_id = '5f88ca1e755f0222f85ce85c'
restclient.get('/policies/%s' % policy_id)
```

Rechercher une politique spécifique avec un identifiant de politique

Ce point terminal recherche la politique spécifiée en utilisant les paramètres d'identifiant de politique comme clé composée.

```
POST /openapi/v1/policies/search
```

Le corps de la requête se compose d'un corps JSON comportant le schéma suivant :

Nom	Type	Description
application_id	chaîne	ID de l'espace de travail de l'application.
policy_identifier	objet	Champs qui constituent l'identifiant cohérent de la politique.

Les champs d'identifiant de politique sont constitués selon le schéma suivant :

Nom	Type	Description
version	chaîne	(Facultatif) Indique la version de l'application pour laquelle obtenir les politiques. utilise par défaut la dernière version « v » de l'application lorsque cela n'est pas spécifié.
consumer_consistent_uuid	chaîne	UUID cohérent du consommateur ou de la source.
provider_consistent_uuid	chaîne	UUID cohérent du fournisseur ou de la destination.
rank	chaîne	Le rang de la politique doit être « DEFAULT (PAR DÉFAUT) » ou « ABSOLUTE (ABSOLUE) ».
action	chaîne	L'action de politique doit être « ALLOW (AUTORISER) » ou « DENY (REFUSER) ».
priority	nombre entier	Valeur de la priorité pour la politique.
protocol	nombre entier	Numéro de protocole IP (0 à 255).
start_port	nombre entier	(Facultatif) Début de la plage de ports (0 à 65 535) la valeur par défaut est 0 lorsqu'elle n'est pas précisée.
end_port	nombre entier	(facultatif) fin de la plage de ports (0 à 65 535); par défaut à 65535 si start_port est égal à 0 ou sinon à start_prot

Exemple de code Python

```
application_id = '5f88ca1e755f0222f85ce85c'
consumer_id = '5f88ca1e755f0222f85ce85d'
provider_id = '5f88ca1e755f0222f85ce85d'
rank = 'DEFAULT'
action = 'ALLOW'
priority = 100
protocol = 6
start_port = 80
version = 'p3'

req_body = f'''
{{
    "application_id": "{application_id}",
    "policy_identifier": {{
        "consumer_consistent_uuid": "{consumer_id}",
        "provider_consistent_uuid": "{provider_id}",
        "rank": "{rank}",
        "action": "{action}",
        "priority": {priority},
        "protocol": "{protocol}",
        "start_port": "{start_port}",
        "version": "{version}"
    }}
}}'''
restclient.post('/policies/search', json_body=req_body)
```

Créer une politique

Ce point terminal est utilisé pour créer de nouvelles politiques.

```
POST /openapi/v1/applications/{application_id}/policies
```

Paramètres :

Attribut	Type	Description
consumer_filter_id	chaîne	ID d'un filtre défini.
provider_filter_id	chaîne	ID d'un filtre défini.
version	chaîne	Indique la version de l'espace de travail dans lequel les politiques doivent être mises à jour.
rank	chaîne	les valeurs peuvent être DEFAULT, ABSOLUTE ou CATCHALL pour le classement
policy_action	chaîne	les valeurs peuvent être ALLOW ou DENY : signifie si nous devons autoriser ou abandonner le trafic du consommateur au fournisseur sur un port de service/protocole donné
priority	nombre entier	Utilisé pour trier les politiques.

Exemple de code Python

```
  req_payload = {
    "version": "v1",
    "rank" : "DEFAULT",
    "policy_action" : "ALLOW",
    "priority" : 100,
    "consumer_filter_id" : "123456789",
    "provider_filter_id" : "987654321",
  }
  resp = restclient.post('/openapi/v1/applications/{application_id}/policies',
json_body=json.dumps(req_payload))
```

Créer une politique par défaut

Ce point terminal est utilisé pour créer de nouvelles politiques par défaut. Ce point terminal crée une politique par défaut semblable à la création d'un point terminal de politique.

```
POST /openapi/v1/applications/{application_id}/default_policies
```

Créer une politique absolue

Ce point terminal est utilisé pour créer de nouvelles politiques absolues. Ce point terminal crée une politique absolue similaire à la création d'un point terminal de politique.

```
POST /openapi/v1/applications/{application_id}/absolute_policies
```

Mettre à jour une politique

Ce point terminal met à jour une politique.

```
PUT /openapi/v1/policies/{policy_id}
```

Paramètres :

Attribut	Type	Description
consumer_filter_id	chaîne	ID d'un filtre défini.
provider_filter_id	chaîne	ID d'un filtre défini.
policy_action	chaîne	Les valeurs possibles peuvent être ALLOW (AUTORISER) ou DENY (REFUSER). Indique si le trafic doit être autorisé ou abandonné pour un port de service ou un protocole entre le consommateur et le fournisseur de service.
priority	nombre entier	Utilisé pour trier les priorités des politiques

Renvoie l'objet de politique modifié associé à l'ID spécifié.

Mettre à jour une politique collectrice

Ce point terminal met à jour la politique Catch All (collectrice) pour un espace de travail particulier.

```
PUT /openapi/v1/applications/{application_id}/catch_all
```

Paramètres :

Attribut	Type	Description
version	chaîne	Indique la version de l'espace de travail dans lequel les politiques doivent être mises à jour.
policy_action	chaîne	Les valeurs possibles peuvent être ALLOW (AUTORISER) ou DENY (REFUSER). Indique si le trafic ne correspondant à aucune des politiques de cet espace de travail sera autorisé ou abandonné.

Ajout de ports de service à une politique

Ce point terminal est utilisé pour créer des ports de service pour une politique spécifique.

```
POST /openapi/v1/policies/{policy_id}/l4_params
```

Paramètres :

Attribut	Type	Description
version	chaîne	Indique la version de l'espace de travail à partir duquel obtenir les politiques.
start_port	nombre entier	Port de début de la plage.
end_port	nombre entier	Port de fin de la plage
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
description	chaîne	(Facultatif) Chaîne courte concernant ce protocole et ce port.

Mise à jour des ports de service d'une politique

Ce point terminal met à jour le port de service spécifié d'une politique.

```
PUT /openapi/v1/policies/{policy_id}/l4_params/{l4_params_id}
```

Paramètres :

Attribut	Type	Description
approved	booléen	Marque la politique comme approuvée.

Suppression des ports de service d'une politique

Ce point terminal supprime le port de service spécifié d'une politique. (Facultatif) Consultez la section Filtres d'exclusion pour en savoir plus.

```
DELETE /openapi/v1/policies/{policy_id}/l4_params/{l4_params_id}
```

Paramètres :

Attribut	Type	Description
create_exclusion_filter	booléen	(Facultatif) Si la valeur est vrai, crée un filtre d'exclusion correspondant à la politique. Les flux correspondant à ce filtre seront exclus des futurs cycles de découverte automatique des politiques. Consultez la section Filtres d'exclusion pour en savoir plus.

Suppression d'une politique

Ce point terminal supprime la politique spécifiée. Aucun filtre d'exclusion n'est créé.

```
DELETE /openapi/v1/policies/{policy_id}
```

Suppression d'une politique avec identifiant

Ce point terminal supprime la politique spécifiée à l'aide des paramètres d'identifiant de politique. Aucun filtre d'exclusion n'est créé.

```
DELETE /openapi/v1/policies/destroy_with_identifier
```

Le corps de la requête se compose d'un corps JSON comportant le schéma suivant :

Nom	Type	Description
application_id	chaîne	ID de l'espace de travail de l'application.
policy_identifier	objet	Champs qui constituent l'identifiant cohérent de la politique.

Les champs d'identifiant de politique sont constitués selon le schéma suivant :

Nom	Type	Description
version	chaîne	(facultatif) la version « v » de l'espace de travail de l'application dans laquelle effectuer l'opération de suppression; utilise par défaut la dernière version « v » de l'espace de travail lorsqu'elle n'est pas précisée.

Nom	Type	Description
consumer_consistent_uuid	chaîne	UUID cohérent du consommateur ou de la source
provider_consistent_uuid	chaîne	UUID cohérent du fournisseur ou de la destination
rank	chaîne	Le rang de la politique doit être « DEFAULT (PAR DÉFAUT) » ou « ABSOLUTE (ABSOLUE) ».
action	chaîne	L'action de politique doit être « ALLOW (AUTORISER) » ou « DENY (REFUSER) ».
priority	nombre entier	Valeur de la priorité pour la politique
protocol	nombre entier	Numéro de protocole IP (0 à 255) de la politique
start_port	nombre entier	(Facultatif) Début de la plage de ports (0 à 65 535) la valeur par défaut est 0 lorsqu'elle n'est pas précisée
end_port	nombre entier	(facultatif) fin de la plage de ports (0 à 65 535); par défaut à 65535 si start_port est égal à 0 ou sinon à start_prot

Exemple de code Python

```
application_id = '5f88ca1e755f0222f85ce85c'
consumer_id = '5f88ca1e755f0222f85ce85d'
provider_id = '5f88ca1e755f0222f85ce85d'
action = 'ALLOW'
rank = 'DEFAULT'
protocol = 6
start_port = 80
priority = 100
version = '5'

req_body = f'''
{{
    "application_id": "{application_id}",
    "policy_identifier": {{
        "consumer_consistent_uuid": "{consumer_id}",
        "provider_consistent_uuid": "{provider_id}",
        "rank": "{rank}",
        "priority": {priority},
        "action": "{action}",
        "protocol": "{protocol}",
        "start_port": "{start_port}",
        "version": "{version}"
```

```
    }}
}}'''
restclient.delete('/policies/destroy_with_identifier', json_body=req_body)
```

Analyse rapide de la politique

Ce point terminal peut être utilisé pour trouver l'ensemble de politiques correspondant à tout flux hypothétique par rapport aux politiques analysées ou appliquées dans une portée racine. Pour plus de détails, consultez Analyse rapide

Cette API est uniquement disponible pour les utilisateurs disposant d'un accès en lecture minimal à la portée racine et nécessite la capacité `app_policy_management` associée à la clé API.

```
POST /openapi/v1/policies/{rootScopeID}/quick_analysis
```

Le corps de la requête se compose d'un corps JSON comportant le schéma suivant :

Nom	Type	Description
consumer_ip	chaîne	Adresse IP du client/consommateur.
provider_ip	chaîne	Adresse IP du serveur/fournisseur.
provider_port	nombre entier	(Facultatif) Port du fournisseur, pertinent uniquement pour les flux TCP ou UDP.
protocol	chaîne	Protocole du flux, par exemple TCP.
analysis_type	chaîne	Le type d'analyse peut être **analyzed (analysé)** ou **enforced (appliqué).** Le type d'analyse « analyzed (analysé) » prend la décision concernant le flux en faisant correspondre ce dernier à toutes les politiques analysées dans la portée racine. Le type d'analyse « enforced (appliqué) » prend la décision du flux en le faisant correspondre à toutes les politiques appliquées dans la portée racine.

Nom	Type	Description
application_id	chaîne	(Facultatif) L'ID de l'espace de travail principal, toujours accompagné dans la version « v » de l'espace de travail, le cas échéant, prend la décision de flux en utilisant les politiques dans la version spécifiée ainsi que les politiques analysées ou appliquées des autres espaces de travail dans la portée racine. Si ce champ est ignoré, la décision du flux est prise en tenant compte de toutes les politiques analysées ou appliquées dans la portée racine.
version	nombre entier	(Facultatif) La version « v » de l'espace de travail mentionnée ci-dessus. Elle doit être spécifiée si application_id est spécifié et doit être ignoré dans le cas inverse.

Exemple de requête

Le corps de la demande doit être une requête au format JSON.

Exemple de corps de requête où la décision de flux est basée sur toutes les politiques analysées :

```
    req_payload = {
        "consumer_ip": "4.4.1.1",
        "provider_ip": "4.4.2.1",
        "provider_port": 9081,
        "protocol": "TCP",
        "analysis_type": "analyzed"
    }
    resp = restclient.post('/openapi/v1/policies/{rootScopeID}/quick_analysis',
json_body=json.dumps(req_payload))
```

Exemple de corps de requête où la décision de flux est basée sur les politiques dans la version « v » de l'espace de travail ainsi que sur les politiques analysées de tous les autres espaces de travail de la portée racine :

```
    req_payload = {
        "consumer_ip": "4.4.1.1",
        "provider_ip": "4.4.2.1",
        "provider_port": 9081,
        "protocol": "TCP",
        "analysis_type": "analyzed",
        "application_id": "5e7e5f56497d4f0bc26c7bb3",
        "version": 1
    }
    resp = restclient.post('/openapi/v1/policies/{rootScopeID}/quick_analysis',
json_body=json.dumps(req_payload))
```

Exemple de réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes

Clés	Valeurs
policy_decision	La décision du flux hypothétique d'autoriser ou de refuser.
outbound_policy	La politique du consommateur qui autorise ou refuse le trafic sortant
inbound_policy	La politique du fournisseur qui autorise ou refuse le trafic entrant


```
{
    "policy_decision": "ALLOW",
    "outbound_policy": {
        "policy_rank": "DEFAULT",
        "start_port": 9082,
        "l4_detail_id": "5e7e600f497d4f7341f4f6d0",
        "src_filter_id": "5e7e600e497d4f7341f4f459",
        "end_port": 9082,
        "cluster_edge_id": "5e7e600f497d4f7341f4f6d1",
        "dst_filter_id": "5e7d0efc497d4f44b6b09351",
        "action": "ALLOW",
        "protocol": "TCP",
        "app_scope_id": "5e7e5f3a497d4f0bc26c7bb0"
    },
    "inbound_policy": {
        "policy_rank": "DEFAULT",
        "start_port": 9082,
        "l4_detail_id": "5e7e600f497d4f7341f4f6d0",
        "src_filter_id": "5e7e600e497d4f7341f4f459",
        "end_port": 9082,
        "cluster_edge_id": "5e7e600f497d4f7341f4f6d1",
        "dst_filter_id": "5e7d0efc497d4f44b6b09351",
        "action": "ALLOW",
        "protocol": "TCP",
        "app_scope_id": "5e7e5f3a497d4f0bc26c7bb0"
    }
}
```


Statistiques de la politique

Ce point terminal renvoie le nombre de paquets, d'octets et de conversations observés pour une politique sur un intervalle de temps. Une conversation peut être décrite dans les grandes lignes comme une observation de flux correspondant à une politique qui est agrégée avec une granularité d'une heure. Le nombre de conversations mesurées pour une politique donnée sur une heure représente le nombre de paires distinctes d'éléments d'inventaire client et fournisseur qui ont communiqué sur le réseau au cours de cette heure.

Bien que ce point terminal accepte les paramètres d'identifiant de politique comme entrées, nous vous recommandons d'utiliser les ID de politique et de paramètres L4 d'une version publiée de l'espace de travail.

Remarque Après la publication d'une nouvelle version de l'espace de travail d'application, six heures peuvent s'écouler avant que les résultats ne soient disponibles. Toutes les résolutions d'horodatage auront également une granularité minimale de 6 heures.

Pour obtenir les statistiques d'une politique sur les versions appliquées d'un espace de travail d'application, le chemin URL est le suivant :

```
POST /openapi/v1/policies/stats/enforced
```

Pour obtenir les statistiques d'une politique sur les versions analysées d'un espace de travail d'application, le chemin URL est le suivant :

```
POST /openapi/v1/policies/stats/analyzed
```

Le corps de la requête se compose d'un corps JSON comportant le schéma suivant :

Tableau 68 :

Nom	Type	Description
application_id	chaîne	ID de l'espace de travail de l'application.
t0	chaîne	Le début de l'intervalle de temps, au format RFC 3339.
t1	chaîne	(facultatif) La fin de l'intervalle de temps au format RFC-3339; correspond par défaut à l'heure actuelle, si elle n'est pas précisée.
policy_id	chaîne	l'ID de la politique; non obligatoire si l'identifiant de politique est présent.
l4_param_id	chaîne	ID du paramètre l4; non obligatoire si l'identifiant de politique est présent, ou pour les politiques « CATCH_ALL ».
policy_identifier	objet	Champs qui constituent l'identifiant cohérent de la politique.

Les champs d'identifiant de politique sont constitués selon le schéma suivant :

Nom	Type	Description
consumer_consistent_uuid	chaîne	UUID cohérent du consommateur ou de la source.
provider_consistent_uuid	chaîne	UUID cohérent du fournisseur ou de la destination.
rank	chaîne	Le rang de la politique doit être « DEFAULT (PAR DÉFAUT) » ou « ABSOLUTE (ABSOLUE) ».
action	chaîne	L'action de politique doit être « ALLOW (AUTORISER) » ou « DENY (REFUSER) ».

Nom	Type	Description
priority	nombre entier	Valeur de la priorité pour la politique.
protocol	nombre entier	Numéro de protocole IP (0 à 255) de la politique.
start_port	nombre entier	(Facultatif) Début de la plage de ports (0 à 65 535) la valeur par défaut est 0 lorsqu'elle n'est pas précisée
end_port	nombre entier	(facultatif) fin de la plage de ports (0 à 65 535); par défaut à 65535 si start_port est égal à 0 ou sinon à start_prot

Exemple de code Python

```
application_id = '5f88ca1e755f0222f85ce85c'
consumer_id = '5f88ca1e755f0222f85ce85d'
provider_id = '5f88ca1e755f0222f85ce85d'
action = 'ALLOW'
rank = 'DEFAULT'
protocol = 6
start_port = 80
priority = 100

req_body = f'''
{{
    "application_id": "{application_id}",
    "t0":"2022-07-06T00:00:00Z",
    "t1":"2022-07-28T19:00:00Z",
    "policy_identifier": {{
        "consumer_consistent_uuid": "{consumer_id}",
        "provider_consistent_uuid": "{provider_id}",
        "rank": "{rank}",
        "priority": {priority},
        "action": "{action}",
        "protocol": "{protocol}",
        "start_port": "{start_port}"
    }}
}}'''
restclient.post('/policies/stats/analyzed', json_body=req_body)

# For CATCH_ALL policies:
root_app_scope_id = '6f88ca1e755f0222f85ce85e'
rank = 'CATCH_ALL'
action = 'DENY'
req_body = f'''
{{
    "application_id": "{application_id}",
    "t0":"2022-07-06T00:00:00Z",
    "t1":"2022-07-28T19:00:00Z",
    "policy_identifier": {{
        "consumer_consistent_uuid": "{root_app_scope_id}",
        "provider_consistent_uuid": "{root_app_scope_id}",
        "rank": "{rank}",
        "action": "{action}"
```

```
    }}
}}'''

restclient.post('/policies/stats/analyzed', json_body=req_body)
```

Exemple de réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Tableau 69 :

Clés	Valeurs
conversation_count	Le nombre de conversations observées pour la durée et la politique spécifiées.
packet_count	Le nombre de paquets observés pour la durée et la politique spécifiées.
byte_count	Le nombre d'octets observés pour la durée et la politique spécifiées.
first_seen_at	Horodatage (au format RFC-3339) de la première observation de flux pour cette politique.
last_seen_at	L'horodatage (au format RFC-3339) de la dernière observation des flux pour cette politique.
agg_start_version	La première version publiée de cette politique enregistrée à partir de l'instant t0.
agg_start_time	Horodatage de publication de agg_start_version.

```
{
  "conversation_count": 72,
  "packet_count": 800,
  "byte_count": 1960,
  "first_seen_at": "2022-09-09T11:00:00.000Z",
  "last_seen_at": "2022-09-09T11:00:00.000Z",
  "agg_start_version": 4,
  "agg_start_time": "2022-08-10T23:00:00.000Z"
}
```

Politiques inutilisées

Ce point terminal renvoie les identifiants de politique dans un espace de travail publié pour lequel aucune conversation n'est observée sur un intervalle de temps spécifié.

Identifiant de la politique

Toutes les politiques et les grappes générées par ADM peuvent modifier leur ID dans les versions de l'espace de travail d'application même si les requêtes de filtre sous-jacentes ou le port et le protocole des politiques ne changent pas. Afin d'assurer le suivi du nombre de résultats pour une politique particulière dans les versions de l'espace de travail, nous utilisons des UUID cohérents pour les filtres qui ne changent pas d'une version à l'autre. Une clé composée appelée *identifiant de politique* comprend des UUID cohérents pour le fournisseur et le consommateur, ainsi que le rang, l'action, la priorité, le port et le protocole.

Ainsi, les identifiants de politiques servent de clé composée qui peut à la fois identifier et décrire les aspects importants d'une politique pour toutes les versions de l'espace de travail d'application, tandis que les ID de politique (comme ceux utilisés dans les points terminaux CRUD habituels) peuvent changer d'une version à l'autre.

Remarque Les UUID et identifiants de politiques cohérents avec le fournisseur ou le consommateur ne permettent pas d'identifier de façon unique un filtre ou une politique, car ils sont partagés entre différentes versions d'espace de travail d'application.

Pour effectuer des opérations CRUD sur une grappe ou une politique particulière, il est recommandé de résoudre l'identifiant à une politique concrète pour une version spécifique de l'espace de travail de l'application, le point d'arrivée de la recherche.

Les opérations CRUD classiques peuvent être effectuées à l'aide des ID de politique, tandis que seuls les statistiques de politique et l'API Détruire avec identifiant acceptent l'identifiant de politique comme entrée. Il s'agit principalement d'éviter l'appel intermédiaire à la recherche et de valider et détruire directement toutes les politiques inutilisées dans un espace de travail.

Il est fortement recommandé d'utiliser les ID de politiques et de filtres dans la mesure du possible et de ne pas générer manuellement des identifiants de politiques pour les points terminaux des statistiques de politique ou de l'API Destroy with Identifier (Détruire avec identifiant). Cependant, l'exemple suivant illustre une façon de générer des identifiants de politiques à partir de l'objet de politiques :

```
resp = restclient.get(f'/policies/631b0590497d4f09b537b973')
policy = resp.json() # policy object
policy_identifer = {
    'consumer_consistent_uuid': policy['consumer_filter']['consistent_uuid'],
    'provider_consistent_uuid': policy['provider_filter']['consistent_uuid'],
    'rank': policy['rank'],
    'action': policy['action'],
    'priority': policy['priority'],
    'protocol': policy['l4_params'][0]['proto'],
    'start_port': policy['l4_params'][0]['port'][0],
    'end_port': policy['l4_params'][0]['port'][1]
}
```

Remarque Après la publication d'une nouvelle version de l'espace de travail d'application, six heures peuvent s'écouler avant que les résultats ne soient disponibles. Toutes les résolutions d'horodatage auront également une granularité minimale de 6 heures.

Pour obtenir les politiques inutilisées des versions appliquées d'un espace de travail d'application, le chemin URL est :

```
POST /openapi/v1/unused_policies/{application_id}/enforced
```

Pour obtenir les politiques inutilisées des versions analysées d'un espace de travail d'application, le chemin URL est :

```
POST /openapi/v1/unused_policies/{application_id}/analyzed
```

Le corps de la requête se compose d'un corps JSON comportant le schéma suivant :

Nom	Type	Description
t0	chaîne	Le début de l'intervalle de temps, au format RFC 3339.
t1	chaîne	(Facultatif) La fin de l'intervalle de temps au format RFC-3339; correspond par défaut à l'heure actuelle, si elle n'est pas précisée.
limit	nombre entier	(Facultatif) Limite le nombre de politiques par demande.
offset	chaîne	(Facultatif) Décalage reçu de la réponse précédente - utile pour la pagination.

```
application_id = '62e1915e755f026f2bcdd805'
resp = restclient.post(f'/unused_policies/{application_id}/analyzed', json_body=f'''
{{
    "t0":"2022-07-06T00:00:00Z",
    "t1":"2022-07-28T19:00:00Z"
}}''')'
```

Exemple de réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Clés	Valeurs
application_id	ID de l'espace de travail de l'application.
policy_identifiers	Une liste des identifiants des politiques inutilisées
offset	Décalage de réponse à transmettre pour la page de résultats suivante.

Pour générer la page de résultats suivante, prenez l'objet reçu par la réponse dans « offset » et transmettez-le comme valeur pour le décalage de la prochaine requête.


```
{
  "application_id": "63054a97497d4f2dc113a9c4",
  "policy_identifiers": [
    {
      "consumer_consistent_uuid": "62fff45c497d4f5064973c4d",
      "provider_consistent_uuid": "62fff45c497d4f5064973c4d",
      "version": "p1",
      "rank": "DEFAULT",
      "policy_action": "ALLOW",
      "priority": 10,
      "proto": 6,
      "start_port": 10000,
      "end_port": 10000,
      "agg_start_version": 1,
      "agg_start_time": "2022-08-10T23:00:00.000Z"
    },
    {
```

```
      "consumer_consistent_uuid": "62fff45c497d4f5064973c4d",
      "provider_consistent_uuid": "62fff45c497d4f5064973c4d",
      "version": "p1",
      "rank": "DEFAULT",
      "policy_action": "ALLOW",
      "priority": 10,
      "protocol": 6,
      "start_port": 10001,
      "end_port": 10001,
      "agg_start_version": 1,
      "agg_start_time": "2022-08-10T23:00:00.000Z"
    }
  ],
  "offset": "eyJvZmZzZXQiOjZ9"
}
```


Modèles de politiques

Cet ensemble d'API peut être utilisé pour ajouter, modifier ou supprimer des modèles de politique et nécessite la capacité app_policy_management associée à la clé API.

Obtenir des modèles de politiques

Ce point terminal renvoie une liste des modèles de politique pour une portée racine particulière. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/application_templates?root_app_scope_id={root_app_scope_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_app_scope_id	chaîne	Identificateur unique de la portée racine.

Objet de réponse : renvoie une liste des objets de modèle de politique pour la portée racine spécifiée.

Exemple de code Python

```
root_app_scope_id = '<root-app-scope-id>'
restclient.get('/application_templates?root_app_scope_id=%s' % root_app_scope_id)
```

Obtenir un modèle de politique spécifique

Ce point terminal renvoie une instance des modèles de politique.

```
GET /openapi/v1/application_templates/{template_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
template_id	chaîne	Identificateur unique du modèle de politique.

Objet de réponse : renvoie l'objet de modèle de politique avec l'ID spécifié.

Exemple de code Python

```
template_id = '<template-id>'
restclient.get('/application_templates/%s' % template_id)
```

Créer un modèle de politique

Ce point terminal est utilisé pour créer un nouveau modèle de politique.

```
POST /openapi/v1/application_templates
```

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
name	chaîne	Utilisé comme nom du modèle lors de l'importation.
description	chaîne	(Facultatif) Description du modèle affichée pendant le processus d'application
paramètres	objet Paramètres	Paramètres du modèle, voir ci-dessous.
absolute_policies	tableau d'objets politiques	(Facultatif) Tableau de politiques absolues.
default_policies	tableau d'objets politiques	(obligatoire) Le tableau de politiques par défaut peut être vide.

Objet de réponse : renvoie l'objet de modèle de politique créé.

Exemple de code Python

```
root_app_scope_id = '<root-app-scope-id>'
payload = {'root_app_scope_id': root_app_scope_id,
           'name': "policy_name",
           'default_policies': [
              {
                'action': 'ALLOW',
                'priority': 100,
                'l4_params': [
                  {
                    'proto': 17,
                    'port': [80, 90]
                  }
                ]
              }
            ]
          }
restclient.post('/application_templates',
                json_body=json.dumps(payload))
```

Mettre à jour un modèle de politique

Ce point terminal met à jour un modèle de politique.

```
PUT /openapi/v1/application_templates/{template_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
template_id	chaîne	Identificateur unique du modèle de politique.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
name	chaîne	(Facultatif) Utilisé comme nom du modèle lors de l'importation.
description	chaîne	(Facultatif) Description du modèle affichée pendant le processus d'application

Objet de réponse : renvoie l'objet de modèle de politique modifié avec l'ID spécifié.

Exemple de code Python

```
new_name = <new-name>
payload = {'name': new_name}
template_id = '<template-id>'
restclient.post('/application_templates/%s' % template_id,
                json_body=json.dumps(payload))
```

Suppression d'un modèle de politique

Ce point terminal supprime le modèle de politique spécifié.

```
DELETE /openapi/v1/application_templates/{template_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
template_id	chaîne	Identificateur unique du modèle de politique.

Objet de réponse : aucun

Exemple de code Python

```
template_id = '<template-id>'
restclient.delete('/application_templates/%s' % template_id)
```

Télécharger un modèle de politique

Ce point terminal télécharge un modèle de politique.

```
GET /openapi/v1/application_templates/{template_id}/download
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
template_id	chaîne	Identificateur unique du modèle de politique.

Objet de réponse : renvoie la définition complète du modèle de politique avec l'ID spécifié.

Exemple de code Python

```
template_id = '<template-id>'
restclient.get('/application_templates/%s/download' % template_id)
```

Grappes

Cet ensemble d'API peut être utilisé pour ajouter, modifier ou supprimer des grappes, qui sont membres d'espaces de travail (« applications »). Ces renseignements nécessitent la capacité `user_role_scope_management` associée à la clé API.

Objet grappe

Les attributs de l'objet grappe sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique de la grappe.
consistent_uuid	chaîne	Un ID cohérent dans toutes les exécutions de découverte automatique des politiques.
application_id	chaîne	ID de l'espace de travail auquel la grappe appartient.
version	chaîne	La version de l'espace de travail à laquelle la grappe appartient
name	chaîne	Nom de la grappe.
description	chaîne	La description de la grappe.
approved	booléen	Si la grappe a été « approuvée » par l'utilisateur .
query	JSON	Filtre (ou critères de correspondance) associé au filtre en conjonction avec les filtres des portées parentes.
short_query	JSON	Filtre (ou critères de correspondance) associé au filtre.

Attribut	Type	Description
alternate_queries	tableau de requêtes	Autres suggestions de requêtes générées par une découverte automatique des politiques exécutée en mode dynamique.
stocks	tableau de l'inventaire	Si demandé, renvoie l'inventaire des membres de la grappe, y compris l'adresse IP, le nom d'hôte, le vrf_id et l'UUID.

Obtenir des grappes

Ce point terminal renvoie la liste des grappes pour un espace de travail (« application ») particulier. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/clusters
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	ID de l'espace de travail auquel la grappe appartient.
version	chaîne	Indique la version de l'espace de travail pour lequel obtenir les grappes.
include_inventory	booléen	Inclure l'inventaire des grappes.

Objet de réponse : renvoie un tableau de toutes les grappes pour cet espace de travail et cette version spécifiques.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
restclient.get('/applications/%s/clusters' % application_id)
```

Obtenir une grappe spécifique

Ce point terminal renvoie une instance d'une grappe.

```
GET /openapi/v1/clusters/{cluster_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
cluster_id	chaîne	Identifiant unique de la grappe.
include_inventory	booléen	Inclure l'inventaire des grappes.

Objet de réponse : renvoie l'objet grappe associé à l'ID spécifié.

Exemple de code Python

```
cluster_id = '5d02d021497d4f0949ba74e4'
restclient.get('/clusters/%s' % cluster_id)
```

Créer une grappe

Ce point terminal est utilisé pour créer une nouvelle grappe.

```
POST /openapi/v1/applications/{application_id}/clusters
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	ID de l'espace de travail auquel la grappe appartient.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
name	chaîne	Nom de la grappe.
version	chaîne	Indique la version de l'espace de travail auquel la grappe sera ajoutée.
description	chaîne	(facultatif) La description de la grappe.
approved	booléen	(Facultatif) Une grappe approuvée ne sera pas mise à jour lors d'une recherche automatique des politiques. La valeur par défaut est faux.
query	JSON	Filtre (ou critères de correspondance) associé au filtre. L'autre mode de requête (également appelé mode dynamique) doit être activé sur l'espace de travail, sinon sera ignoré.
query	JSON	Filtre (ou critères de correspondance) associé au filtre. L'autre mode de requête (également appelé mode dynamique) doit être activé sur l'espace de travail, sinon sera ignoré.

Attribut	Type	Description
nœuds	Tableau	Liste des adresses IP ou des points terminaux. Sera utilisé pour créer la requête correspondant à ces adresses IP, sauf si une requête est fournie et que l'espace de travail est en mode dynamique.

Attributs de l'objet nœud :

Nom	Type	Description
ip	chaîne	Adresse IP
name	chaîne	(Facultatif) Le nom du nœud.
prefix_len	nombre entier	(Facultatif) Masque de sous-réseau.

Note Les nœuds seront utilisés pour créer une requête, sauf si une requête est fournie et que l'espace de travail est en mode dynamique.

Objet de réponse : renvoie l'objet de grappe nouvellement créé.

Exemple de code Python

```
application_id = '5d02b493755f0237a3d6e078'
payload = {
  'name': 'test_cluster',
  'version': 'v2',
  'description': 'basic granularity',
  'approved': False,
  'query': {
      'type': 'eq',
      'field': 'host_name',
      'value': 'centos6001'
  }
}
restclient.post('/applications/%s/clusters' % application_id)
```

Mettre à jour une grappe

Ce point terminal met à jour une grappe.

```
PUT /openapi/v1/clusters/{cluster_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
cluster_id	chaîne	Identifiant unique de la grappe.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
name	chaîne	Nom de la grappe.
description	chaîne	(facultatif) La description de la grappe.
approved	booléen	Une grappe approuvée ne sera pas mise à jour lors d'une exécution de découverte automatique des politiques.
query	JSON	Filtre (ou critères de correspondance) associé au filtre. L'autre mode de requête (également appelé mode dynamique) doit être activé sur l'espace de travail, sinon sera ignoré.

Objet de réponse : renvoie l'objet de grappe modifié associé à l'ID spécifié.

Exemple de code Python

```
cluster_id = '5d02d2a4497d4f5194f104ef'
payload = {
  'name': 'new_test_cluster',
}
restclient.put('/clusters/%s' % cluster_id, json_body=json.dumps(payload))
```

Suppression d'une grappe

Ce point terminal supprime la grappe spécifiée. Si la grappe est utilisée par une politique, la grappe ne sera pas supprimée et une liste des entités dépendantes sera renvoyée.

```
DELETE /openapi/v1/clusters/{cluster_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
cluster_id	chaîne	Identifiant unique de la grappe.

Objet de réponse : aucun

Exemple de code Python

```
cluster_id = '5d02d2a4497d4f5194f104ef'
restclient.delete('/clusters/%s' % cluster_id)
```

Conversations

Les conversations sont des flux agrégés dans la plage temporelle d'une exécution de découverte automatique de politique où le port consommateur est supprimé. Vous trouverez une description plus détaillée des conversations dans la section Conversations.

Cette API vous permet de rechercher les conversations générées lors d'une exécution de découverte automatique des politiques pour un espace de travail donné. Elle nécessite la capacité `app_policy_management` associée à la clé API pour appeler cette API.

Rechercher des conversations dans une exécution de découverte de politiques

Ce point de terminaison vous permet de rechercher les conversations dans une exécution de découverte automatique des politiques pour un espace de travail donné. Vous pouvez également spécifier un sous-ensemble de dimensions et de mesures prises en charge que vous souhaitez peut-être voir dans les conversations téléchargées. Vous pouvez également rechercher un sous-ensemble de conversations en utilisant des filtres sur les dimensions et les statistiques prises en charge.

```
POST /openapi/v1/conversations/{application_id}
```

La requête consiste en un corps JSON avec les clés suivantes.

Nom	Type	Description
version	nombre entier	Version de l'exécution de découverte automatique des politiques
filter	JSON	(Facultatif) Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à toutes les conversations. Des conversations plus spécifiques peuvent être téléchargées en utilisant des filtres sur les dimensions et les mesures prises en charge. Pour la syntaxe des filtres, reportez-vous à la section Filtres .
dimensions	tableau	(facultatif) Liste des dimensions à renvoyer pour les conversations téléchargées. La liste des dimensions prises en charge se trouve Dimensions prises en charge .
metrics	tableau	(Facultatif) Liste des paramètres à renvoyer pour les conversations téléchargées. La liste des mesures prises en charge se trouve Mesures prises en charge .
limit	nombre entier	(Facultatif) Nombre de conversations à afficher dans une seule réponse d'API.
offset	chaîne	(Facultatif) Décalage reçu de la réponse précédente : utile pour la pagination.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "version": 1,
    "filter": {
        "type": "and",
        "filters":[
            {
                "type": "eq",
                "field": "excluded",
                "value": False
            },
            {
                "type": "eq",
                "field": "protocol",
                "value": "TCP"
            },
        ]
    },
    "dimensions": ["src_ip", "dst_ip", "port"],
    "metrics": ["byte_count", "packet_count"],
    "limit" : 2,
    "offset": <offset-object>
}
```

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Clés	Valeurs
offset	Décalage de réponse à transmettre pour la page de résultats suivante
results	Liste des résultats

Pour générer la page de résultats suivante, prenez l'objet reçu par la réponse dans « `offset` » et transmettez-le comme valeur pour le `décalage` de la prochaine requête.

```
   req_payload = {"version": 1,
                  "limit": 10,
                  "filter": {"type": "and",
                      "filters": [
                          {"type": "eq", "field": "excluded", "value": False},
                          {"type": "eq", "field": "protocol", "value": "TCP"}
                       ]
                  }
    }

    resp = restclient.post('/conversations/{application_id}',
json_body=json.dumps(req_payload))
    print resp.status_code
    if resp.status_code == 200:
        parsed_resp = json.loads(resp.content)
        print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

N principales conversations dans une exécution de découverte de politiques

Ce point terminal vous permet de rechercher dans les principales conversations une découverte automatique des politiques exécutée pour un espace de travail donné en fonction d'une mesure et regroupées par dimension. Les mesures actuellement prises en charge sont Mesures prises en charge et les groupes par dimensions actuellement pris en charge sont Dimensions prises en charge vous pouvez interroger un sous-ensemble de conversations en utilisant des filtres sur les dimensions et les mesures prises en charge. Par exemple, vous pouvez rechercher l'adresse IP source avec le plus grand nombre de conversations de trafic d'octets en utilisant une requête avec la dimension `src_ip` et la mesure `byte_count`.

```
POST /openapi/v1/conversations/{application_id}/topn
```

La requête consiste en un corps JSON avec les clés suivantes.

Nom	Type	Description
version	nombre entier	Version de l'exécution de découverte automatique des politiques
dimension	chaîne	La dimension selon laquelle les conversations doivent être regroupées pour les N premières requêtes. Dimensions prises en charge : src_ip, dst_ip
metric	chaîne	La mesure de tri des N principales conversations. La liste des mesures prises en charge se trouve Mesures prises en charge .
filter	JSON	(Facultatif) Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à toutes les conversations. Des conversations plus spécifiques peuvent être téléchargées en utilisant des filtres sur les dimensions et les mesures prises en charge. Pour la syntaxe des filtres, consultez la section Filtres .
seuil	nombre entier	Nombre des N principaux résultats à renvoyer dans une seule réponse API.

Le corps de la demande doit être au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "version": 1,
    "dimension": "src_ip",
    "metric": "byte_count",
    "filter": {
```

```
            "type": "and",
            "filters":[
                {
                    "type": "eq",
                    "field": "excluded",
                    "value": False
                },
                {
                    "type": "eq",
                    "field": "protocol",
                    "value": "TCP"
                },
            ]
        },
        "threshold" : 10
    }
```

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Clés	Valeurs
results	Liste avec un objet JSON avec une clé de résultats et une valeur d'une liste d'objets de résultats avec des clés correspondant à la dimension et à la mesure de la requête.

```
  [ {"result": [
    {
      "byte_count": 1795195565,
      "src_ip": "192.168.1.6"
    },
    {
      "byte_count": 1781002379,
      "src_ip": "192.168.1.28"
    },
    ...
  ] } ]
```

```
    req_payload = {"version": 1, "dimension": "src_ip", "metric": "byte_count",
      "filter": {"type": "and",
        "filters": [
          {"type": "eq", "field": "excluded", "value": False},
          {"type": "eq", "field": "protocol", "value": "TCP"},
         {"type": "eq", "field": "consumer_filter_id", "value": "16b12a5614c5af5b68afa7ce"},

          {"type": "subnet", "field": "src_ip", "value": "192.168.1.0/24"}
        ]
      },
      "threshold" : 10
    }

    resp = restclient.post('/conversations/{application_id}/topn',
json_body=json.dumps(req_payload))
    print resp.status_code
    if resp.status_code == 200:
        parsed_resp = json.loads(resp.content)
        print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Dimensions prises en charge

Nom	Type	Description
src_ip	chaîne	Adresse IP du consommateur
dst-ip	chaîne	Adresse IP du fournisseur
protocol	chaîne	Protocole utilisé dans la communication. Ex : « TCP », « UDP », etc.
port	nombre entier	Port du fournisseur.
address_type	chaîne	« IPv4 » ou « IPv6 »
consumer_filter_id	chaîne	ID de grappe de la grappe si l'adresse IP du consommateur appartient à une grappe, sinon l'ID de portée auquel l'adresse IP du consommateur appartient.
provider_filter_id	chaîne	ID de grappe de la grappe si l'adresse IP du fournisseur appartient à une grappe, sinon l'ID de la portée auquel l'adresse IP du fournisseur appartient.
excluded	booléen	Indique si cette conversation est exclue lors de la génération des politiques.
confidence	double	Le niveau de confiance de la classification des consommateurs et des fournisseurs. La valeur varie de 0,0 à 1,0, 1,0 étant la classification la plus sûre.

Mesures prises en charge

Nom	Type	Description
byte_count	nombre entier	Nombre total d'octets dans la conversation
packet_count	nombre entier	Nombre total de paquets dans la conversation

Filtres d'exclusion

Cet ensemble d'API peut être utilisé pour ajouter, modifier ou supprimer des filtres d'exclusion et nécessiter la capacité `user_role_scope_management` associée à la clé API.

Les filtres d'exclusion excluent les flux de l'algorithme de mise en grappe de la découverte automatique des politiques. Consultez la section Filtres d'exclusion pour en savoir plus.

Objet filtre d'exclusion

Les attributs de l'objet du filtre d'exclusion sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique de la grappe.
application_id	chaîne	ID de l'espace de travail auquel le filtre d'exclusion appartient.
version	chaîne	La version de l'espace de travail à laquelle appartient le filtre d'exclusion.
consumer_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme consommateur d'une politique.
provider_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme fournisseur d'une politique.
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	tableau	Gamme de ports inclusive. ex., [80, 80] ou [5000, 6000]. NULL signifie tous les ports.
updated_at	nombre entier	Horodatage Unix de la mise à jour du filtre d'exclusion.

Obtenir les filtres d'exclusion

Ce point terminal renvoie une liste des filtres d'exclusion pour un espace de travail particulier. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/applications/{application_id}/exclusion_filters
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.
version	chaîne	Indique la version de l'espace de travail pour lequel obtenir les filtres d'exclusion.

Objet de réponse : renvoie une liste des objets filtre d'exclusion pour l'espace de travail et la version spécifiés.

Exemple de code Python

```
application_id = '<application-id>'
params = {'version': 'v10'}
restclient.get('/applications/%s/exclusion_filters' % application_id,
               params=params)
```

Obtenir un filtre d'exclusion spécifique

Ce point terminal renvoie une instance de filtres d'exclusion.

```
GET /openapi/v1/exclusion_filters/{exclusion_filter_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion.

Objet de réponse : renvoie l'objet de filtre d'exclusion avec l'ID spécifié.

Exemple de code Python

```
exclusion_filter_id = '<exclusion-filter-id>'
restclient.get('/exclusion_filters/%s' % exclusion_filter_id)
```

Créer un filtre d'exclusion

Ce point terminal est utilisé pour créer un nouveau filtre d'exclusion.

```
POST /openapi/v1/applications/{application_id}/exclusion_filters
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
application_id	chaîne	Identificateur unique de l'espace de travail.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
version	chaîne	La version de l'espace de travail à laquelle appartient le filtre d'exclusion.

Attribut	Type	Description
consumer_filter_id	chaîne	(Facultatif) ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme consommateur d'une politique.
provider_filter_id	chaîne	(Facultatif) ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme fournisseur d'une politique.
proto	nombre entier	(Facultatif) Valeur entière du protocole (NULL signifie tous les protocoles).
start_port	nombre entier	(Facultatif) Port de début de la plage.
end_port	nombre entier	(Facultatif) Port de fin de la plage.

Les paramètres facultatifs manquants seront considérés comme des caractères génériques (correspondent à n'importe lequel).

Objet de réponse : renvoie l'objet filtre d'exclusion créé.

Exemple de code Python

```
provider_filter_id = '<provider-filter-id>'
consumer_filter_id = '<consumer-filter-id>'
payload = {'version': 'v0',
           'consumer_filter_id': consumer_filter_id,
           'provider_filter_id': provider_filter_id,
           'proto': 6,
           'start_port': 800,
           'end_port': 1000}
application_id = '<application-id>'
restclient.post('/applications/%s/exclusion_filters' % application_id,
                json_body=json.dumps(payload))
```

Mettre à jour un filtre d'exclusion

Ce point terminal met à jour un filtre d'exclusion.

```
PUT /openapi/v1/exclusion_filters/{exclusion_filter_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
consumer_filter_id	chaîne	(Facultatif) ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme consommateur d'une politique.
provider_filter_id	chaîne	(Facultatif) ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme fournisseur d'une politique.
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
start_port	nombre entier	(Facultatif) Port de début de la plage.
end_port	nombre entier	(Facultatif) Port de fin de la plage.

Objet de réponse : renvoie l'objet de filtre d'exclusion modifié avec l'ID spécifié.

Exemple de code Python

```
payload = {'proto': 17}
exclusion_filter_id = '<exclusion-filter-id>'
restclient.post('/exclusion_filters/%s' % exclusion_filter_id,
                json_body=json.dumps(payload))
```

Suppression d'un filtre d'exclusion

Ce point terminal supprime le filtre d'exclusion spécifié.

```
DELETE /openapi/v1/exclusion_filters/{exclusion_filter_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion.

Objet de réponse : aucun

Exemple de code Python

```
exclusion_filter_id = '<exclusion-filter-id>'
restclient.delete('/exclusion_filters/%s' % exclusion_filter_id)
```

Filtres d'exclusion par défaut

Cet ensemble d'API peut être utilisé pour ajouter, modifier ou supprimer des filtres d'exclusion par défaut et nécessiter la capacité `app_policy_management` associée à la clé API.

Les filtres d'exclusion excluent les flux de l'algorithme de mise en grappe de la découverte automatique des politiques. Consultez la section Filtres d'exclusion pour en savoir plus.

Objet filtre d'exclusion par défaut

Les attributs de l'objet du filtre d'exclusion sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique du filtre d'exclusion par défaut.
consumer_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme consommateur d'une politique.
provider_filter_id	chaîne	ID d'un filtre défini. Actuellement, toute grappe appartenant à l'espace de travail, au filtre défini par l'utilisateur ou à la portée peut être utilisée comme fournisseur d'une politique.
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
port	tableau	Gamme de ports inclusive. ex., [80, 80] ou [5000, 6000]. NULL signifie tous les ports.
updated_at	nombre entier	Horodatage Unix de la mise à jour du filtre d'exclusion.

Obtenir les filtres d'exclusion par défaut

Ce point terminal renvoie une liste de filtres d'exclusion par défaut. Cette API est disponible pour les clés API avec la capacité `app_policy_management`.

```
GET /openapi/v1/default_exclusion_filters?root_app_scope_id={root_app_scope_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_app_scope_id	chaîne	Identificateur unique de la portée racine.

Objet de réponse : renvoie une liste des objets de filtre d'exclusion par défaut pour la portée racine.

Exemple de code Python

```
root_app_scope_id = '<root-app-scope-id>'
 restclient.get('/default_exclusion_filters?root_app_scope_id=%s' % root_app_scope_id)
```

Obtenir un filtre d'exclusion par défaut spécifique

Ce point terminal renvoie une instance de filtres d'exclusion par défaut.

```
default_exclusion_filter_id = '<default-exclusion-filter-id>'

restclient.get('/default_exclusion_filters/%s' % default_exclusion_filter_id)
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
default_exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion.

Objet de réponse : renvoie l'objet de filtre d'exclusion par défaut avec l'ID précisé.

Exemple de code Python

```
default_exclusion_filter_id = '<default-exclusion-filter-id>'
restclient.get('/default_exclusion_filters/%s' % default_exclusion_filter_id)
```

Créer un filtre d'exclusion par défaut

Ce point terminal est utilisé pour créer un nouveau filtre d'exclusion par défaut.

```
POST /openapi/v1/default_exclusion_filters?root_app_scope_id={root_app_scope_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_app_scope_id	chaîne	Identificateur unique de la portée racine.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
consumer_filter_id	chaîne	(facultatif) ID d'une portée ou d'un inventaire défini.
provider_filter_id	chaîne	(facultatif) ID d'une portée ou d'un inventaire défini.
proto	nombre entier	(facultatif) Valeur entière de protocole (NULL signifie tous les protocoles).
start_port	nombre entier	(Facultatif) Port de début de la plage.

Attribut	Type	Description
end_port	nombre entier	(Facultatif) Port de fin de la plage.

Objet de réponse : renvoie l'objet filtre d'exclusion par défaut créé.

Exemple de code Python

```
provider_filter_id = '<provider-filter-id>'
consumer_filter_id = '<consumer-filter-id>'
payload = {'consumer_filter_id': consumer_filter_id,
           'provider_filter_id': provider_filter_id,
           'proto': 6,
           'start_port': 800,
           'end_port': 1000}
root_app_scope_id = '<root-app-scope-id>'
restclient.post('/default_exclusion_filters?root_app_scope_id=%s' % root_app_scope_id,
                json_body=json.dumps(payload))
```

Mettre à jour un filtre d'exclusion par défaut

Ce point terminal met à jour un filtre d'exclusion par défaut.

```
PUT /openapi/v1/default_exclusion_filters/{default_exclusion_filter_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
default_exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion par défaut.

Le corps de la requête JSON contient les clés suivantes :

Attribut	Type	Description
consumer_filter_id	chaîne	(facultatif) L'ID d'une portée ou d'un filtre d'inventaire défini.
provider_filter_id	chaîne	(facultatif) L'ID d'une portée ou d'un filtre d'inventaire défini.
proto	nombre entier	Valeur entière du protocole (NULL signifie tous les protocoles).
start_port	nombre entier	(Facultatif) Port de début de la plage.
end_port	nombre entier	(Facultatif) Port de fin de la plage.

Objet de réponse : renvoie l'objet de filtre d'exclusion par défaut modifié avec l'ID précisé.

Exemple de code Python

```
payload = {'proto': 17}
default_exclusion_filter_id = '<default-exclusion-filter-id>'
```

```
restclient.post('/default_exclusion_filters/%s' % default_exclusion_filter_id,
                json_body=json.dumps(payload))
```

Suppression d'un filtre d'exclusion par défaut

Ce point terminal supprime le filtre d'exclusion par défaut spécifié.

```
DELETE /openapi/v1/default_exclusion_filters/{default_exclusion_filter_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
default_exclusion_filter_id	chaîne	Identificateur unique du filtre d'exclusion.

Objet de réponse : aucun

Exemple de code Python

```
default_exclusion_filter_id = '<default-exclusion-filter-id>'
restclient.delete('/default_exclusion_filters/%s' % default_exclusion_filter_id)
```

Analyse en temps réel

L'analyse en direct (dite aussi en temps réel) ou l'analyse des politiques est un aspect important de la génération de politiques de sécurité. Elle vous permet d'évaluer l'incidence d'un ensemble de politiques (lorsqu'elles sont générées par la découverte automatique des politiques ou ajoutées manuellement par les utilisateurs) avant d'appliquer réellement ces politiques sur les charges de travail. L'analyse en direct permet aux utilisateurs d'exécuter une analyse de simulation sur le trafic en direct sans perturber le trafic des applications.

L'ensemble d'API disponibles dans cette section permet le téléchargement de flux et de l'effet de l'ensemble actuel de politiques publiées dans un espace de travail sur ces flux. La capacité `app_policy_management` de la clé API est nécessaire pour appeler cet ensemble d'API.

Les flux disponibles via l'analyse en direct ont certains attributs (dimensions et mesures) et l'API de téléchargement permet à l'utilisateur de filtrer les flux en fonction de différents critères sur les dimensions.

Dimensions de flux disponibles dans l'analyse en temps réel

Ce point terminal est utile pour connaître les colonnes sur lesquelles les critères de recherche (ou *filtres*) peuvent être spécifiés pour le téléchargement des flux disponibles via l'analyse en direct. Le scénario d'utilisation le plus courant serait de télécharger des flux *permitted (autorisés)*, *escaped (échappés)* ou *rejected (rejetés)* . Il est possible d'y parvenir en transmettant à l'API de téléchargement un critère de recherche sur la dimension de la catégorie. Lorsque l'API est utilisée avec **type: eq**, les catégories entrantes et sortantes du flux doivent correspondre. Utilisé avec **type: contains** la catégorie des flux entrants ou sortants doit correspondre

```
GET /openapi/v1/live_analysis/dimensions
```

Indicateurs de flux disponibles dans l'analyse en temps réel

Ce point terminal renvoie la liste des mesures (p. ex., nombre d'octets, nombre de paquets) associées à l'analyse en direct. Un scénario d'utilisation de ce point terminal consisterait à projeter un sous-ensemble de mesures

dans l'API de téléchargement, c'est-à-dire qu'au lieu de télécharger toutes les mesures, les utilisateurs peuvent spécifier un sous-ensemble plus restreint de mesures qui les intéressent.

```
GET /openapi/v1/live_analysis/metrics
```

Télécharger les flux disponibles via l'analyse en temps réel

Ce point terminal renvoie la liste des flux correspondant aux critères de filtre. Chaque objet de flux dans le résultat possède des attributs qui sont une union des dimensions d'analyse en direct (renvoyées par l'API des dimensions d'analyse en direct ci-dessus) ainsi que des mesures d'analyse en direct (renvoyées par l'API des métriques d'analyse en direct ci-dessus). Si vous le souhaitez, l'utilisateur peut également préciser un petit sous-ensemble de dimensions ou de métriques s'il n'est pas intéressé par l'ensemble complet de dimensions et de métriques disponibles. Cette prévision d'un sous-ensemble plus petit de dimensions ou de métriques a également pour effet secondaire d'accélérer les appels d'API.

```
POST /openapi/v1/live_analysis/{application_id}
```

Le corps de la requête se compose d'un corps JSON avec les clés suivantes.

Nom	Type	Description
t0	entier ou chaîne	Début de l'intervalle de temps (heure d'origine ou ISO 8601)
t1	entier ou chaîne	Fin de l'intervalle de temps (heure d'origine ou ISO 8601)
filter	JSON	Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à tous les flux. Reportez-vous à la section sur les Filtres dans la recherche de flux pour connaître la syntaxe des filtres.
dimensions	tableau	(facultatif) Liste des dimensions de flux à renvoyer pour les flux téléchargés, disponible par le biais de l'analyse en direct. Si ce n'est pas spécifié, toutes les dimensions disponibles sont affichées.
metrics	tableau	(facultatif) Liste des mesures de flux à renvoyer pour les flux téléchargés, disponible par le biais de l'analyse en direct.
limit	nombre entier	(facultatif) Nombre de flux à renvoyer en une seule réponse API.
offset	chaîne	(Facultatif) Décalage reçu de la réponse précédente : utile pour la pagination.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "t0": "2016-06-17T09:00:00-0700",
    "t1": "2016-06-17T17:00:00-0700",
    "filter": {
        "type": "and",
        "filters": [
            {
                "type": "contains",
                "field": "category",
                "value": "escaped"
            },
            {
                "type": "in",
                "field": "dst_port",
                "values": ["80", "443"]
            }
        ]
    },
    "limit": 100,
    "offset": <offset-object>
}
```

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Clés	Valeurs
offset	Décalage de réponse à transmettre pour la page de résultats suivante
results	Liste des résultats

Pour générer la page de résultats suivante, prenez l'objet reçu par la réponse dans « `offset` » et transmettez-le comme valeur pour le `décalage` de la prochaine requête.

Exemple de code Python

```
   req_payload = {"t0": "2016-11-07T09:00:00-0700",
                  "t1": "2016-11-07T19:00:00-0700",
                  "limit": 10,
                  "filter": {"type": "and",
                      "filters": [
                          {"type": "contains", "field": "category", "value": "escaped"},
                          {"type": "regex", "field": "src_hostname", "value": "web*"}
                       ]
                  }
    }

    resp = restclient.post('/live_analysis/{application_id}',
json_body=json.dumps(req_payload))
    print resp.status_code
    if resp.status_code == 200:
        parsed_resp = json.loads(resp.content)
        print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Portées

Cet ensemble d'API peut être utilisé pour gérer les portées (ou AppScopes) au sein de déploiement de grappes Cisco Secure Workload. Ces renseignements nécessitent la capacité `user_role_scope_management` associée à la clé API. L'API pour obtenir la liste des portées est également disponible pour les clés API avec la capacité `app_policy_management` ou `sensor_management`.

Objet portée

Les attributs de l'objet portée sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique de la portée.
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
name	chaîne	Nom complet du domaine de la portée. Il s'agit d'un nom complet, c'est-à-dire qu'il comporte le nom des portées parentes (le cas échéant) jusqu'à la portée racine.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.
query	JSON	Le filtre (ou les critères de correspondance) associé à la portée conjointement avec les filtres des portées parents (jusqu'à la portée racine).
vrf_id	nombre entier	ID du VRF auquel la portée appartient.
parent_app_scope_id	chaîne	ID de la portée parente.
child_app_scope_ids	tableau	Un tableau d'ID d'enfants de la portée.
policy_priority		Utilisé pour trier les priorités de l'espace de travail. Reportez-vous à la section Attributs de la politique.
dirty	booléen	Indique qu'une requête parent ou enfant a été mise à jour et que les modifications doivent être validées.

Attribut	Type	Description
dirty_short_query	JSON	Non NULL si la requête pour cette portée a été mise à jour mais n'est pas encore validée.

Obtenir les portées

Ce point terminal renvoie une liste des portées connues de l'appareil Cisco Secure Workload. Cette API est disponible pour les clés API avec la capacité `app_policy_management` ou `user_role_scope_management`.

```
GET /openapi/v1/app_scopes
```

Paramètres :

Nom	Type	Description
vrf_id	nombre entier	Correspondance des portées d'application en fonction de l'identifiant vrf_id.
root_app_scope_id	chaîne	Correspondance des portées d'application en fonction de l'identifiant de la portée de l'application racine.
exact_name	chaîne	Renvoie la portée correspondant au nom exact, en respectant la casse.
exact_short_name	chaîne	Renvoie les portées correspondant exactement à short_name, en respectant la casse.

Renvoie la liste des objets de la portée.

Créer une portée

Ce point terminal est utilisé pour créer de nouvelles portées.

```
GET /openapi/v1/app_scopes
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.

Nom	Type	Description
parent_app_scope_id	chaîne	ID de la portée parente.
policy_priority	nombre entier	La valeur par défaut est « dernier ». Utilisé pour trier les priorités de l'espace de travail. Voir l'ordonnancement des politiques sous Consulter les politiques découvertes automatiquement.

Exemple de code Python

```
 req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "parent_app_scope_id": <parent_app_scope_id>
}
resp = restclient.post('/app_scopes', json_body=json.dumps(req_payload))
```

Pour créer une portée en fonction du sous-réseau, utilisez la commande short_query suivante :

```
  "short_query":
    {
      "type":"subnet",
      "field":"ip",
      "value": "1.0.0.0/8"
    },
```

Obtenir une portée spécifique

Ce point terminal renvoie une instance d'une portée.

```
GET /openapi/v1/app_scopes/{app_scope_id}
```

Renvoie l'objet de portée associé à l'ID spécifié.

Mettre à jour une portée

Ce point terminal met à jour une portée. Les modifications apportées au `nom` et à la `description` sont appliquées immédiatement. Les modifications apportées à short_query marquent la portée comme « dirty » (sale) et définissent l'attribut « `dirty_court_query` ». Une fois que toutes les modifications de requête de portée, dans une portée racine donnée, sont effectuées, il faut envoyer un message ping au point de terminaison Valider les modifications de requête de portée (Valider les modifications de requête de portée) pour valider toutes les mises à jour requises.

```
PUT /openapi/v1/app_scopes/{app_scope_id}
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.

Renvoie l'objet de portée modifié associé à l'ID spécifié.

Supprimer une portée spécifique

Ce point terminal supprime la portée spécifiée.

```
DELETE /openapi/v1/app_scopes/{app_scope_id}
```

Si la portée est associée à un espace de travail, à une politique, à un filtre d'inventaire utilisateur, etc., ce point terminal renverra `422 Unprocessable Entity` (422 Entité non traitable). L'objet Erreur renvoyé contiendra un attribut `détails` avec le nombre d'objets dépendants ainsi que les identifiants des 10 premiers de chaque type. Ces renseignements peuvent être utilisés pour localiser et supprimer les dépendances bloquantes.

Obtenir les portées par ordre de priorité des politiques

Ce point terminal répertorie les portées dans l'ordre dans lequel leur espace de travail principal correspondant sera mis en application.

```
POST /openapi/v1/app_scopes/ {root_app_scope_id}/politique_commande
```

Renvoie un tableau des objets de la portée.

Mettre à jour l'ordre de la politique

Ce point terminal mettra à jour l'ordre dans lequel les politiques sont appliquées.

Warning Ce point terminal modifie l'ordre dans lequel les politiques sont appliquées. Par conséquent, de nouvelles règles de pare-feu hôte seront insérées et toutes les règles existantes seront supprimées sur les hôtes concernés.

```
POST /openapi/v1/app_scopes/ {root_app_scope_id}/politique_commande
```

Paramètres :

Nom	Type	Description
root_app_scope_id	chaîne	Portée racine ou dont l'ordre est en cours de modification.

Nom	Type	Description
ids	tableau	un tableau de chaînes d'ID de portée dans l'ordre dans lequel elles doivent être appliquées.

Le paramètre de tableau `ids` doit inclure tous les membres de la portée racine, y compris la racine.

Valider les modifications de requête de portée

Ce point terminal déclenche une tâche en arrière-plan asynchrone pour mettre à jour tous les enfants « modifiés » d'une portée racine donnée. Cette tâche met à jour les portées et les espaces de travail. Portées pour plus de détails.

```
POST /openapi/v1/app_scopes/commit_dirty
```

Paramètres :

Nom	Type	Description
root_app_scope_id	chaîne	ID d'une portée racine dont tous les enfants seront mis à jour.
sync	booléen	(Facultatif) Indiquez si la requête doit être synchrone.

Renvoie 202 pour indiquer que la tâche a été mise en file d'attente. Pour vérifier si la tâche est terminée, interrogez l'attribut « dirty » de la portée racine pour voir s'il a été défini sur faux.

Les utilisateurs peuvent transmettre le paramètre `sync` (synchronisation) pour que la tâche soit exécutée immédiatement. La demande sera renvoyée une fois terminée avec un code d'état 200. Cette demande peut prendre un certain temps si de nombreuses mises à jour doivent être appliquées.

Envoyer une demande de suggestions de groupe

Envoyer une demande de suggestions de groupe pour une porter.

```
PUT /openapi/v1/app_scopes/{app_scope_id}/suggest_groups
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
app_scope_id	chaîne	Identificateur unique pour la portée.

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
start_time	chaîne	Heure de début de l'intervalle de saisie de suggestions de groupe.
end_time	chaîne	Heure de fin de l'intervalle de saisie de suggestions de groupe.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
message	chaîne	Message concernant la réussite ou l'échec de l'envoi de la demande de suggestions de groupe.

Exemple de code Python

```
app_scope_id = '5d02b493755f0237a3d6e078'
req_payload = {
      'start_time': '2020-09-17T10:00:00-0700',
      'end_time': '2020-09-17T11:00:00-0700',
}
resp = restclient.put('/app_scopes/%s/suggest_groups' % app_scope_id,
                      json_body=json.dumps(req_payload))
```

Obtenir l'état de la proposition de groupe

Interroger l'état de proposition de groupe de la portée.

```
GET /openapi/v1/app_scopes/{app_scope_id}/suggest_groups_status
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
app_scope_id	chaîne	Identificateur unique pour la portée.

Objet de réponse : renvoie un objet avec les attributs suivants :

Nom	Type	Description
état	chaîne	État de la proposition de groupe Valeurs : PENDING (EN COURS), COMPLETE (TERMINÉ) ou FAILED (ERREUR)

Exemple de code Python

```
app_scope_id = '5d02b493755f0237a3d6e078'
resp = restclient.get('/app_scopes/%s/suggest_groups_status' % app_scope_id)
```

Configurer les alertes

Cet ensemble d'API peut être utilisé pour gérer les alertes d'utilisateurs. Elles nécessitent la capacité `user_alert_management` associée à la clé API.

Objet alerte

Chaque objet de configuration d'alerte contient les champs suivants :

Attribut	Type	Description
app_name	chaîne	Nom de l'application associée à la configuration d'alerte.
règles	objet	Ensemble de conditions qui doivent être respectées pour que la configuration des alertes déclenche une alerte.
subjects	objet	Liste des utilisateurs qui doivent recevoir l'alerte.
gravité	chaîne	Indique le niveau de gravité associé à une configuration d'alerte.
individual_alert	booléen	Indique si des alertes individuelles doivent être envoyées pour déclencher la configuration des alertes.
summary_alert_freq	chaîne	Fréquence des résumés d'alertes à envoyer pour une configuration d'alerte particulière.
alert_type	chaîne	Identifiant unique de la configuration d'alerte.
app_instance_id	chaîne	Identifiant unique d'une instance particulière associée à la configuration d'alerte

Recevoir des alertes

Ce point terminal récupère la liste des configurations d'alertes pour un utilisateur. Les alertes peuvent être filtrées selon une portée racine donnée. Si aucune portée n'est fournie, toutes les alertes sont renvoyées pour toutes les portées auxquelles l'utilisateur a accès. Les alertes du fournisseur de services ne seront renvoyées que si l'utilisateur est un administrateur du site.

```
GET /openapi/v1/alert_confs
```

Paramètres :

Nom	Type	Description
root_app_scope_id	chaîne	(Facultatif) ID d'une portée racine pour renvoyer les alertes uniquement affectées à cette portée.

Objet de réponse : renvoie une liste des objets d'alerte de l'utilisateur.

Créer une alerte

Ce point terminal est utilisé pour créer une nouvelle alerte.

```
POST openapi/v1/alert_confs
```

Paramètres :

Attribut	Type	Description
app_name	chaîne	Nom de l'application associée à la configuration d'alerte.
règles	objet	Ensemble de conditions qui doivent être respectées pour que la configuration des alertes déclenche une alerte.
subjects	objet	Liste des utilisateurs qui doivent recevoir l'alerte.
gravité	chaîne	Indique le niveau de gravité associé à une configuration d'alerte.
individual_alert	booléen	Indique si des alertes individuelles doivent être envoyées pour déclencher la configuration des alertes.
summary_alert_freq	chaîne	Fréquence des résumés d'alertes à envoyer pour une configuration d'alerte particulière.
alert_type	chaîne	Identifiant unique de la configuration d'alerte.
app_instance_id	chaîne	Identifiant unique d'une instance particulière associée à la configuration d'alerte.

L'utilisateur demandeur doit avoir accès à la portée fournie. Une alerte sans portée est une « alerte de fournisseur de services », et seul un administrateur de site peut en créer.

Objet de réponse : renvoie l'objet alerte nouvellement créé.

Obtenir une alerte spécifique

Ce point terminal renvoie un objet d'alerte spécifique.

```
GET /openapi/v1/alert_confs/
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
alert_id	chaîne	Identifie de façon unique l'alerte.

Objet de réponse : renvoie un objet d'alerte associé à l'ID précisé.

Mettre à jour une alerte

Ce point terminal est utilisé pour mettre à jour une alerte existante.

```
PUT /openapi/v1/alert_confs/
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
alert_id	chaîne	Pour récupérer ou modifier les paramètres de configuration de l'alerte,

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Nom spécifié par l'utilisateur pour l'alerte.
description	chaîne	Description fournie par l'utilisateur pour l'alerte.

L'utilisateur demandeur doit avoir accès à la portée fournie. Une alerte sans portée est appelée une « alerte de fournisseur de services » et seul l'administrateur du site peut la mettre à jour.

Objet de réponse : objet d'alerte mis à jour avec l'ID spécifié.

Supprimer une alerte spécifique

Ce point terminal supprime l'alerte spécifiée.

```
DELETE /openapi/v1/alert_confs/{alert_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
alert_id	chaîne	Identifie de façon unique l'alerte.

Objet de réponse : aucun.

Rôles

Cet ensemble d'API peut être utilisé pour gérer les rôles d'utilisateur. Ces renseignements nécessitent la capacité `user_role_scope_management` associée à la clé API.

Note Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

Objet rôle

Les attributs d'objets de rôle sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique du rôle
app_scope_id	chaîne	Portée à laquelle la portée est définie, peut-être vide pour « Rôles de fournisseur de services ».
name	chaîne	Nom indiqué par l'utilisateur pour le rôle.
description	chaîne	Description définie par l'utilisateur pour le rôle.

Obtenir des rôles

Ce point terminal renvoie une liste des rôles accessibles à l'utilisateur. Les rôles peuvent être filtrés selon une portée racine donnée. Si aucune portée n'est fournie, tous les rôles sont retournés, pour toutes les portées auxquelles l'utilisateur a accès. Les rôles de fournisseur de services ne seront renvoyés que si l'utilisateur est un administrateur de site.

```
GET /openapi/v1/roles
```

Paramètres :

Nom	Type	Description
app_scope_id	chaîne	(Facultatif) ID d'une portée racine pour renvoyer les rôles uniquement affectés à cette portée.

Objet de réponse : renvoie une liste des objets rôle d'utilisateur.

Exemple de code Python

```
resp = restclient.get('/roles')
```

Créer un rôle

Ce point terminal est utilisé pour créer un nouveau rôle.

```
POST /openapi/v1/roles
```

Paramètres :

Nom	Type	Description
name	chaîne	Nom indiqué par l'utilisateur pour le rôle.
description	chaîne	Description définie par l'utilisateur pour le rôle.
app_scope_id	chaîne	(Facultatif) L'ID de portée sous lequel le rôle est créé. Si aucun ID de portée n'est mentionné, le rôle est considéré comme un rôle de fournisseur de services.

L'utilisateur demandeur doit avoir accès à la portée fournie. Un rôle sans portée est appelé « rôle de fournisseur de services » et seul l'administrateur du site peut le créer.

Objet de réponse : renvoie l'objet rôle nouvellement créé.

Exemple de code Python

```
app_scope_id = '<app-scope-id>'
req_payload = {
      'name': 'Role Name',
      'description': 'Role Description',
      'app_scope_id': app_scope_id
}
restclient.post('/roles', json_body=json.dumps(req_payload))
```

Obtenir un rôle spécifique

Ce point terminal renvoie un objet de rôle spécifique.

```
GET /openapi/v1/roles/{role_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	Permet d'identifier le rôle de façon unique.

Objet de réponse : renvoie un objet de rôle associé à l'ID spécifié.

Exemple de code Python

```
role_id = '<role-id>'
restclient.get('/roles/%s' % role_id)
```

Mettre à jour un rôle

Ce point terminal est utilisé pour mettre à jour un rôle existant.

```
PUT /openapi/v1/roles/{role_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	Permet d'identifier le rôle de façon unique.

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Nom indiqué par l'utilisateur pour le rôle.
description	chaîne	Description définie par l'utilisateur pour le rôle.

L'utilisateur demandeur doit avoir accès à la portée fournie. Un rôle sans portée est appelé « rôle de fournisseur de services » et seul l'administrateur du site peut le mettre à jour.

Objet de réponse : l'objet rôle mis à jour avec l'ID précisé.

Exemple de code Python

```
role_id = '<role-id>'
req_payload = {
      'name': 'Role Name',
      'description': 'Role Description',
}
restclient.put('/roles/%s' % role_id, json_body=json.dumps(req_payload))
```

Accorder l'accès à un rôle à la portée

Ce point terminal donne à un rôle le niveau d'accès spécifié à une portée.

```
POST /openapi/v1/roles/ {role_id}/capabilities
```

Les capacités ne peuvent être ajoutées qu'aux rôles auxquels l'utilisateur a accès. Si le rôle est affecté à une portée, les capacités doivent correspondre à cette portée ou à ses enfants. Les rôles de fournisseur de services (ceux qui ne sont affectés à aucune portée) peuvent ajouter des fonctionnalités à n'importe quelle portée.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	Permet d'identifier le rôle de façon unique.

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
app_scope_id	chaîne	ID de la portée pour laquelle l'accès est fourni.

Nom	Type	Description
ability	chaîne	Les valeurs possibles sont SCOPE_READ, SCOPE_WRITE, EXECUTE, ENFORCE, SCOPE_OWNER, DEVELOPER

Pour obtenir une description plus détaillée des capacités, reportez-vous à la section Rôles .

Objet de réponse :

Nom	Type	Description
app_scope_id	chaîne	ID de la portée pour laquelle l'accès est fourni.
id_rôle	chaîne	ID du rôle.
ability	chaîne	Les valeurs possibles sont SCOPE_READ, SCOPE_WRITE, EXECUTE, ENFORCE, SCOPE_OWNER, DEVELOPER
inherited	booléen	

Exemple de code Python

```
role_id = '<role-id>'
req_payload = {
  'app_scope_id': '<app-scope-id>',
  'ability': 'SCOPE_READ'
}
restclient.post('/roles/%s/capabilities' % role_id,
                json_body=json.dumps(req_payload))
```

Supprimer un rôle spécifique

Ce point terminal supprime le rôle spécifié.

```
DELETE /openapi/v1/roles/{role_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	Permet d'identifier le rôle de façon unique.

Objet de réponse : aucun.

Exemple de code Python

```
role_id = '<role-id>'
restclient.delete('/roles/%s' % role_id)
```

Utilisateurs

Cet ensemble d'API gère les utilisateurs. Ces renseignements nécessitent la capacité `user_role_scope_management` associée à la clé API.

Note Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

Objet utilisateur

Les attributs de l'objet utilisateur sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique du rôle
e-mail	chaîne	Adresse de courriel associée au compte d'utilisateur.
first_name	chaîne	Prénom
last_name	chaîne	Nom
app_scope_id	chaîne	La portée à laquelle l'utilisateur est affecté. Peut-être vide si l'utilisateur est un « utilisateur de fournisseur de services ».
role_ids	liste	Liste des ID des rôles affectés au compte d'utilisateur.
by-pass_external_auth	booléen	Vrai pour les utilisateurs locaux et faux pour les utilisateurs d'authentification externes (LDAP ou SSO).
disabled_at	nombre entier	Horodatage Unix du moment où l'utilisateur a été désactivé. Zéro ou nul, sinon.

Obtenir des utilisateurs

Ce point terminal renvoie une liste des objets utilisateur connus de l'appareil Cisco Secure Workload.

```
GET /openapi/v1/users
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
include_disabled	booléen	(Facultatif) Pour inclure les utilisateurs désactivés, la valeur par défaut est False.
app_scope_id	chaîne	(Facultatif) Renvoie uniquement les utilisateurs affectés à la portée fournie.

Objet de réponse : renvoie une liste des objets utilisateur. Seuls les administrateurs de site peuvent voir les utilisateurs du fournisseur de services, c.-à-d. ceux qui ne sont affectés à aucune portée.

Exemple de code Python

```
GET /openapi/v1/users
```

Créer un nouveau compte utilisateur

Ce point terminal est utilisé pour créer un nouveau compte d'utilisateur.

`POST /openapi/v1/users`

Paramètres : le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
e-mail	chaîne	Adresse de courriel associée au compte d'utilisateur.
first_name	chaîne	Prénom
last_name	chaîne	Nom
app_scope_id	chaîne	(Facultatif) Portée racine à laquelle l'utilisateur appartient.
role_ids	liste	(Facultatif) La liste des rôles à attribuer à l'utilisateur.

L'app_scope_id est l'ID de la portée racine à laquelle l'utilisateur doit être affecté. Si app_scope_id n'est pas présent, l'utilisateur est un « utilisateur de fournisseur de services ». Seuls les administrateurs de site peuvent créer des utilisateurs fournisseurs de services. Les `value_ids` sont les ID des rôles qui ont été créés dans la portée d'application spécifiée.

Objet de réponse : renvoie l'objet utilisateur nouvellement créé.

Exemple de code Python

```
req_payload = {
    "first_name": "fname",
    "last_name": "lname",
    "email": "foo@bar.com"
    "app_scope_id": "root_appscope_id",
```

```
    "role_ids": ["roleid1", "roleid2"]
}
resp = restclient.post('/users', json_body=json.dumps(req_payload))
```

Obtenir un utilisateur spécifique

Ce point terminal renvoie un objet utilisateur spécifique.

```
GET /openapi/v1/users/{user_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur.

Objet de réponse : renvoie un objet utilisateur associé à l'ID spécifié.

Exemple de code Python

```
user_id = '5ce480db497d4f1ca1fc2b2b'
resp = restclient.get('/users/%s' % user_id)
```

Mettre à jour un utilisateur

Ce point terminal met à jour un utilisateur existant.

```
PUT /openapi/v1/users/{user_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur en cours de mise à jour.

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
e-mail	chaîne	Adresse de courriel associée au compte d'utilisateur.
first_name	chaîne	Prénom
last_name	chaîne	Nom
app_scope_id	chaîne	ID de portée de l'application racine (autorisé uniquement pour les administrateurs de site)

Objet de réponse : renvoie l'objet utilisateur nouvellement mis à jour.

Exemple de code Python

```
req_payload = {
    "first_name": "fname",
    "last_name": "lname",
```

```
    "email": "foo@bar.com"
    "app_scope_id": "root_appscope_id",
}
restclient.put('/users', json_body=json.dumps(req_payload))
```

Activer ou réactiver un utilisateur désactivé

Ce point terminal est utilisé pour réactiver un utilisateur désactivé.

```
POST /openapi/v1/users/{user_id}/enable
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur qui est activé.

Objet de réponse : renvoie l'objet utilisateur réactivé associé à l'ID spécifié.

Exemple de code Python

```
user_id = '5ce480db497d4f1ca1fc2b2b'
resp = restclient.post('/users/%s/enable' % user_id)
```

Ajouter un rôle au compte d'utilisateur

Ce point terminal est utilisé pour ajouter un rôle à un compte d'utilisateur.

```
PUT /openapi/v1/users/{user_id}/add_role
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur en cours de modification.

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	ID de l'objet de rôle à ajouter.

Objet de réponse : renvoie l'objet utilisateur modifié associé à l'ID spécifié.

Exemple de code Python

```
user_id = '5ce480db497d4f1ca1fc2b2b'
req_payload = {
    "role_id": "5ce480d4497d4f1c155d0cef",
}
resp = restclient.put('/users/%s/add_role' % user_id,
                      json_body=json.dumps(req_payload))
```

Supprimer le rôle du compte d'utilisateur

Ce point terminal est utilisé pour supprimer un rôle d'un compte d'utilisateur.

```
DELETE /openapi/v1/users/{user_id}/remove_role
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur en cours de suppression.

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
id_rôle	chaîne	ID de l'objet rôle à supprimer.

Objet de réponse : renvoie l'objet utilisateur modifié associé à l'ID spécifié.

Exemple de code Python

```
user_id = '5ce480db497d4f1ca1fc2b2b'
req_payload = {
    "role_id": "5ce480d4497d4f1c155d0cef",
}
resp = restclient.delete('/users/%s/remove_role' % user_id,
                         json_body=json.dumps(req_payload))
```

Supprimer un utilisateur spécifique

Ce point terminal supprime le compte d'utilisateur spécifié.

```
DELETE /openapi/v1/users/{user_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
user_id	chaîne	ID de l'objet utilisateur en cours de suppression.

Objet de réponse : renvoie l'objet utilisateur supprimé associé à l'ID spécifié.

Exemple de code Python

```
user_id = '5ce480db497d4f1ca1fc2b2b'
resp = restclient.delete('/users/%s' % user_id)
```

Filtres d'inventaire

Les filtres d'inventaire codent les critères de correspondance pour les requêtes de recherche d'inventaire. Cet ensemble d'API fournit des fonctionnalités similaires à celles décrites dans les Filtres d'inventaire. Ils nécessitent la capacité `sensor_management ou app_policy_management` associée à la clé API.

Objet filtre d'inventaire

L'objet JSON du filtre d'inventaire est renvoyé sous forme d'objet unique ou de tableau d'objets selon le point de terminaison d'API. Les attributs de l'objet sont décrits ci-dessous :

Attribut	Type	Description
ID	chaîne	Identifiant unique du filtre d'inventaire.
name	chaîne	Nom spécifié par l'utilisateur pour le filtre d'inventaire.
app_scope_id	chaîne	ID de la portée associée au filtre.
short_query	JSON	Filtre (ou critères de correspondance) associé au filtre.
principal	booléen	Lorsque la valeur est « vrai », le filtre est limité à la portée de la propriété.
public	booléen	Lorsqu'il est défini sur « vrai », le filtre fournit un service pour sa portée. Doit également être principal ou de portée limitée.
query	JSON	Filtre (ou critères de correspondance) associé au filtre en conjonction avec les filtres des portées parentes. Ces conjonctions prennent effet si la case « restricted to ownership scope » (limité à la portée de la propriété) est cochée. Si le champ « primary » (principal) est faux, la requête est identique à short_query.

Obtenir des filtres d'inventaire

Ce point terminal renvoie une liste des filtres d'inventaire visibles par l'utilisateur.

```
POST /openapi/v1/filters/inventories
```

Paramètres :

Nom	Type	Description
vrf_id	nombre entier	Mettre en correspondance les filtres d'inventaire par ID de VRF.
root_app_scope_id	chaîne	Faire correspondre les filtres d'inventaire par ID de portée de l'application racine.
name	chaîne	Renvoie les filtres d'inventaire correspondant à une partie du nom, insensible à la casse.
exact_name	chaîne	Renvoie les filtres d'inventaire correspondant au nom exact, sensibles à la casse.

Créer un filtre d'inventaire

Ce point terminal est utilisé pour créer un filtre d'inventaire.

```
POST /openapi/v1/filters/inventories
```

Paramètres :

Nom	Type	Description
name	chaîne	Nom spécifié par l'utilisateur pour la portée de l'application.
query	JSON	Filtre (ou critères de correspondance) associé au filtre.
app_scope_id	chaîne	ID de la portée associée au filtre.
principal	booléen	Lorsque la valeur est « vrai », le filtre est limité à la portée de la propriété.
public	booléen	Lorsqu'il est défini sur « vrai », le filtre fournit un service pour sa portée. Il doit également s'agir d'un domaine principal ou d'une portée restreinte.

Exemple de code Python

```
req_payload = {
  "app_scope_id": <app_scope_id>,
  "name": "sensor_config_inventory_filter",
  "query": {
    "type": "eq",
    "field": "ip",
    "value": <sensor_interface_ip>
```

```
  },
}
resp = restclient.post('/filters/inventories', json_body=json.dumps(req_payload))
```

Valider une requête de filtre d'inventaire

Ce point terminal validera la structure d'une requête par rapport au schéma requis.

```
POST /openapi/v1/filters/inventories/validate_query
```

Paramètres :

Nom	Type	Description
query	JSON	Filtre (ou critères de correspondance) associé à la portée.

Objet de réponse :

Attribut	Type	Description
valide	booléen	Indique si la requête est valide
erreurs	tableau	Si non valide, détails sur les erreurs

Obtenir un filtre d'inventaire spécifique

Ce point terminal renvoie une instance d'un filtre d'inventaire.

```
GET /openapi/v1/filters/inventories/{inventory_filter_id}
```

Renvoie un objet de filtre d'inventaire associé à l'ID spécifié.

Mettre à jour un filtre d'inventaire spécifique

Ce point terminal est utilisé pour mettre à jour un filtre d'inventaire.

```
PUT /openapi/v1/filters/inventories/{inventory_filter_id}
```

Paramètres :

Nom	Type	Description
name	chaîne	Nom spécifié par l'utilisateur de la portée.
query	JSON	Filtre (ou critères de correspondance) associé à la portée.
app_scope_id	chaîne	ID de la portée associée au filtre.
principal	booléen	Lorsque la valeur est « vrai », le filtre est limité à la portée de la propriété.

Nom	Type	Description
public	booléen	Lorsqu'il est défini sur « vrai », le filtre fournit un service. Peut être utilisé dans le cadre de la génération de politiques. Il doit également s'agir d'un domaine principal ou d'une portée restreinte.
Utilisations	booléen	Collecte des statistiques de politique et de configuration des membres.

Supprimer un filtre d'inventaire en particulier

Ce point terminal supprime le filtre d'inventaire spécifié.

```
GET /openapi/v1/filters/inventories/{inventory_filter_id}
```

Recherche de flux

La fonction de recherche de flux offre des fonctionnalités similaires à celles décrites dans la section Flux de réseau – Visibilité du trafic. Ces ensembles d'API nécessitent la capacité `flow_inventory_query` associée à la clé API.

Requête de dimensions de flux

Ce point terminal renvoie la liste des colonnes de flux dans lesquelles des critères de recherche (ou *filtres*) peuvent être spécifiés pour les requêtes de recherche de flux (ci-dessous). Pour en savoir plus sur les descriptions de colonnes, consultez Colonnes et filtres.

```
GET /openapi/v1/flowsearch/dimensions
```

Paramètres : Aucun

Objet de réponse :

Nom	Type	Description
dimensions	Liste de chaînes	La liste des dimensions téléchargées par l'utilisateur et l'orchestrateur.

Exemple de code Python

```
restclient.get('/flowsearch/dimensions')
```

Requête de mesures de flux

Ce point terminal renvoie la liste des mesures, par exemple le nombre d'octets et le nombre de paquets, associées aux observations de flux.

```
GET /openapi/v1/flowsearch/métriques
```

Paramètres : Aucun

Objet de réponse :

Nom	Type	Description
metrics	Liste de chaînes.	Liste des mesures disponibles.

Exemple de code Python

```
restclient.get('/flowsearch/metrics')
```

Requête de flux

Ce point terminal renvoie la liste des flux correspondant aux critères de filtre. Chaque objet de flux dans le résultat possède des attributs qui sont une union des dimensions de flux (renvoyées par l'API des dimensions de flux ci-dessus) ainsi que des mesures de flux (renvoyées par l'API des mesures de flux ci-dessus).

```
POST /openapi/v1/flowsearch
```

La liste des colonnes qui peuvent être spécifiées dans les critères de filtre peut être obtenue à l'aide de l'API `/openapi/v1/flowsearch/ dimensions`.

Paramètres : le corps de la requête se compose d'un corps JSON avec les clés suivantes.

Nom	Type	Description
t0	entier ou chaîne	Heure de début de la recherche de flux (heure d'origine ou ISO 8601)
t1	entier ou chaîne	Heure de fin de la recherche de flux (heure d'origine ou ISO 8601)
filter	JSON	Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à tous les flux.
scopeName	chaîne	Nom complet de la portée à laquelle la requête est limitée.

Nom	Type	Description
dimensions	tableau	(Facultatif) Liste des noms de dimensions à renvoyer dans le résultat de l'API flowsearch. Il s'agit d'un paramètre facultatif. Si ce paramètre n'est pas spécifié, les résultats de la recherche de flux renvoient toutes les dimensions disponibles. Cette option est utile pour spécifier un sous-ensemble des dimensions disponibles lorsque l'appelant ne se soucie pas du reste des dimensions.
metrics	tableau	(Facultatif) Liste des noms de mesures à renvoyer dans le résultat de l'API flowsearch. Il s'agit d'un paramètre facultatif. Si ce paramètre n'est pas spécifié, les résultats de la recherche de flux renvoient toutes les mesures disponibles. Cette option est utile pour spécifier un sous-ensemble de mesures disponibles lorsque l'appelant n'est pas intéressé par le reste des mesures.
limit	nombre entier	(Facultatif) Limite du nombre de flux de réponse.
offset	chaîne	(Facultatif) Objet décalage reçu de la réponse précédente.
descending	booléen	(Facultatif) Si ce paramètre est défini sur « faux » ou non défini, les résultats sont classés dans l'ordre ascendant des horodatages. Si la valeur du paramètre est « vrai », les résultats sont classés dans l'ordre décroissant des horodatages.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "t0": "2016-06-17T09:00:00-0700",
    "t1": "2016-06-17T17:00:00-0700",
    "filter": {
        "type": "and",
        "filters": [
            {
```

```
                "type": "contains",
                "field": "dst_hostname",
                "value": "prod"
            },
            {
                "type": "in",
                "field": "dst_port",
                "values": ["80", "443"]
            }
        ]
    },
    "scopeName": "Default:Production:Web",
    "limit": 100,
    "offset": <offset-object>
}
```

Filtres

Le filtre prend en charge les filtres primaires et les filtres logiques (« not », « and », « or ») composés d'un ou de plusieurs filtres primaires. Le format du filtre primaire est le suivant :

```
{"type" : "<OPERATOR>", "field": "<COLUMN_NAME>", "value": "<COLUMN_VALUE>"}
```

Pour les filtres primaires , l'opérateur peut être un opérateur de comparaison comme `eq, ne, lt, lte, gt` ou `gte`. L'operateur peut également être `in, regex, subnet, contains` ou `range`.

Voici quelques exemples de filtres primaires :

```
{"type": "eq", "field": "src_address", "value": "7.7.7.7"}

{"type": "regex", "field": "src_hostname", "value": "prod.*"}

{"type": "subnet", "field": "src_addr", "value": "1.1.11.0/24"}

# Note, 'in' clause uses 'values' key instead of 'value'
{"type": "in", "field": "src_port", "values": [80, 443]}
```

Vous pouvez également spécifier des filtres complexes à l'aide d'opérations booléennes telles que not", "and" ou "or". Voici quelques exemples de ces types de filtres :

```
 # "and" and "or" operators need to specify list of "filters"
 {"type": "and",
     "filters": [
         {"type": "in", "field": "src_port", "values": [80, 443]},
         {"type": "regex", "field": "src_hostname", "value": "prod.*"}
     ]
 }

 # "not" operator needs to specify a "filter"
 {"type": "not",
     "filter": {"type": "subnet", "field": "src_addr", "value": "1.1.11.0/24"}
 }
```

Plus formellement, le schéma du `filtre` dans la demande de recherche de flux est le suivant :

Clés	Valeurs
type	Type de filtre
Champ	Colonne du champ de filtre pour les filtres primaires

Clés	Valeurs
filter	Objet filtre (utilisé uniquement pour le type de filtre `not`)
filtres	Liste des objets filtre (utilisés pour les types de filtres `and` et `or`)
valeur	Valeur des filtres primaires
values (valeurs)	Liste de valeurs pour les filtres primaires avec le type de filtre `in` ou `range`

Types de filtres primaires

eq, ne : recherche dans les flux l'égalité ou l'inégalité, respectivement, dans la colonne spécifiée par « `field` » (champ) avec la valeur spécifiée par « `value` » (valeur). Prend en charge les champs suivants : `src_hostname, dst_hostname, src_address, dst_address, src_port, dst_port, src_scope_name, dst_scope_name, vrf_name, src_enforcement_epg_name, dst_enforcement_epg_name, proto`. Ces opérateurs fonctionnent également sur les colonnes étiquetées par l'utilisateur.

lt, lte, gt, gte : recherche les flux où les valeurs de la colonne spécifiées par « `field` » sont inférieures, égales, supérieures ou égales à (selon le cas) la valeur spécifiée par « `value` ». Prend en charge les champs suivants : `[src_port, dst_port]`.

range(plage) : recherche les flux pour les valeurs de la colonne spécifiées par « field » entre le début et la fin de la plage spécifiée par la liste « values » (cette liste doit être de taille 2 pour le type de filtre *« range »* : la première valeur est le début de la plage et la deuxième est la fin de plage). Prend en charge les champs suivants : [src_port, dst_port].

in : recherche les flux pour les membres dans la colonne spécifiée par « `field` » dans la liste de membres spécifiée par « `values` ». Prend en charge les champs suivants : `src_hostname, dst_hostname, src_address, dst_address, src_port, dst_port, src_scope_name, dst_scope_name, vrf_name, src_enforcement_epg_name, dst_enforcement_epg_name, proto`. Cet opérateur fonctionne également sur les colonnes étiquetées par l'utilisateur.

regex, contains : recherche dans les flux les correspondances d'expressions régulières ou les correspondances de stockage, respectivement, dans la colonne spécifiée par « `field` » avec l'expression régulière spécifiée par « `value` ». Prend en charge les champs suivants : `src_hostname, dst_hostname, src_scope_name, dst_scope_name, vrf_name, src_enforcement_epg_name, dst_enforcement_epg_name`. Ces opérateurs fonctionnent également sur les colonnes étiquetées par l'utilisateur. Les filtres de type `regex (expression régulière)` doivent utiliser des modèles d'expression régulière de style Java comme « `valeur` ».

subnet : recherche les flux pour les membres de sous-réseau spécifiés par « `field` » sous forme de chaîne en notation CIDR. Prend en charge les champs suivants : `["src_address", "dst_address"]`

Types de filtres logiques

- **not** : filtre « non » logique de l'objet spécifié par « `filtre` ».
- **and** : filtre « et » logique de la liste des objets de filtre spécifiées par « `filtres` ».
- **or** : filtre « ou » logique de la liste des objets de filtre spécifiés par « `filtres` ».

Objet de réponse :

Clés	Valeurs
offset	Décalage de réponse à transmettre pour la page de résultats suivante
results	Liste des résultats

Pour générer la page de résultats suivante, prenez l'objet reçu par la réponse dans « `offset` » et transmettez-le comme valeur pour le `décalage` de la prochaine requête.

Exemple de code Python

```
req_payload = {"t0": "2016-11-07T09:00:00-0700",
               "t1": "2016-11-07T19:00:00-0700",
               "scopeName": "Default:Prod:Web",
               "limit": 10,
               "filter": {"type": "and",
                   "filters": [
                    {"type": "subnet", "field": "src_address", "value": "1.1.11.0/24"},

                       {"type": "regex", "field": "src_hostname", "value": "web*"}
                    ]
               }
}

resp = restclient.post('/flowsearch', json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Requête TopN pour les flux

Ce point terminal renvoie une liste des N valeurs triées les plus hautes d'une dimension spécifiée, où le rang dans la liste est déterminé par l'agrégation de la métrique spécifiée.

`POST /openapi/v1/flowsearch/topn`

Paramètres :

La liste des colonnes qui peuvent être spécifiées dans les critères de filtre peut être obtenue à l'aide de l'API `/openapi/v1/flowsearch/dimensions`. Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous. Les paramètres `t0` et `t1` du corps de la demande peuvent être au format heure d'origine ou au format ISO 8601. L'API TopN permet uniquement d'interroger une plage temporelle maximale d'un jour. La dimension selon laquelle le regroupement doit être effectué doit être précisée dans le champ `Dimension`. La mesure selon laquelle les N premiers résultats doivent être classés doit être spécifiée dans le champ de `mesure` dans le corps JSON. Vous devez spécifier un `seuil` avec une valeur minimale de 1, ce qui signifie le « N » de « TopN ». La valeur maximale de ce `seuil` est 1 000. Même si l'utilisateur spécifie plus de 1000, l'API ne renvoie qu'un maximum de 1000 résultats. En outre, vous devez spécifier un paramètre appelé `scopeName` qui correspond au nom complet de la portée à laquelle vous souhaitez restreindre la recherche. Le `filtre` est le même que celui du filtre de recherche de flux Filtres, on page 1020 . Si le `filtre` n'est pas mentionné, topN est appliqué à toutes les entrées d flux.e

```
{
  "t0": "2016-06-17T09:00:00-0700",    # t0 can also be 1466179200
  "t1": "2016-06-17T17:00:00-0700",    # t1 can also be 1466208000
  "dimension": "src_address",
```

```
    "metric": "fwd_pkts",
   "filter": {"type": "eq", "field": "src_address", "value": "172.29.203.193"},  #optional

    "threshold": 5,
    "scopeName": "Default"
  }
```

Le corps de la requête se compose d'un corps JSON avec les clés suivantes.

Clés	Valeurs
t0	Heure de début du flux (heure d'origine ou ISO 8601)
t1	Heure de fin du flux (heure d'origine ou ISO 8601)
filter	Filtre de requête. Si le filtre est vide (c.-à-d. {}) ou le filtre est absent (facultatif), la requête topN est appliquée à toutes les entrées de flux
scopeName	Nom complet de la portée à laquelle la requête est limitée
dimension	La dimension est un champ sur lequel nous regroupons.
metric	La mesure est le nombre total de valeurs de la dimension.
seuil	Le seuil est N dans le N top.

Objet de réponse :

Clés	Valeurs
résultat	Tableau des N principales entrées

Exemple de code Python

```
req_payload = {
    "t0": "2017-06-07T08:20:00-07:00",
    "t1": "2017-06-07T14:20:00-07:00",
    "dimension": "src_address",
    "metric": "fwd_pkts",
    "filter": {"type": "ne", "field": "src_address", "value": "172.29.203.193"},
    "threshold": 5,
    "scopeName": "Default"
}
resp = rc.post('/flowsearch/topn',
               json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse

```
[
  { "result": [
    {"src_address": "172.31.239.163", "fwd_pkts": 23104},
```

```
    {"src_address": "172.31.239.162", "fwd_pkts": 22410},
    {"src_address": "172.31.239.166", "fwd_pkts": 16185},
    {"src_address": "172.31.239.168", "fwd_pkts": 15197},
    {"src_address": "172.31.239.169", "fwd_pkts": 15116}
    ]
  }
]
```

Nombre de flux

Ce point terminal renvoie le nombre d'observations de flux correspondant aux critères spécifiés.

`POST /openapi/v1/flowsearch/count`

Paramètres :

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous. Les paramètres `t0` et `t1` du corps de la demande peuvent être au format heure d'origine ou au format ISO 8601. Cette API permet uniquement d'interroger une plage temporelle maximale d'un jour. En outre, vous devez spécifier le paramètre `scopeName` qui correspond au nom complet de la portée à laquelle vous souhaitez restreindre la recherche. Si ce paramètre n'est pas spécifié, la demande API de comptage des observations de flux s'applique à toutes les portées auxquelles vous avez un accès en lecture. Le `filtre` est identique à celui du filtre de recherche de flux Filtres (Filtres).

```
{
  "t0": "2016-06-17T09:00:00-0700",    # t0 can also be 1466179200
  "t1": "2016-06-17T17:00:00-0700",    # t1 can also be 1466208000
  "filter": {"type": "eq", "field": "src_address", "value": "172.29.203.193"},
  "scopeName": "Default"
}
```

Le corps de la requête se compose d'un corps JSON avec les clés suivantes.

Clés	Valeurs
t0	Heure de début du flux (heure d'origine ou ISO 8601)
t1	Heure de fin du flux (heure d'origine ou ISO 8601)
filter	Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à tous les flux.
scopeName	Nom complet de la portée à laquelle la requête est limitée

Objet de réponse :

Clés	Valeurs
Nombre	Le nombre d'observations de flux correspondant aux critères de recherche de flux.

Exemple de code Python

```
req_payload = {
      "t0": "2017-07-20T08:20:00-07:00",
      "t1": "2017-07-20T10:20:00-07:00",
      "scopeName": "Tetration",
```

```
      "filter": {
                  "type": "eq",
                  "field": "dst_port",
                  "value": "5642"
              }
}
resp = rc.post('/flowsearch/count',
               json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse

```
{"count":508767}
```

Inventaire

Les API de recherche d'inventaire fournissent des fonctionnalités similaires à celles décrites dans la section Recherche d'inventaire. Ces ensembles d'API nécessitent la capacité `flow_inventory_query` associée à la clé API.

Requête de dimensions d'inventaire

Ce point terminal renvoie la liste des colonnes d'inventaire sur lesquelles des critères de recherche (ou des *filtres*) peuvent être spécifiés pour réaliser les requêtes de recherche d'inventaire.

```
GET /openapi/v1/inventory/search/dimensions
```

Recherche dans l'inventaire

Ce point terminal renvoie la liste des éléments de l'inventaire correspondant aux critères spécifiés.

```
POST /openapi/v1/inventory/search
```

La liste des colonnes qui peuvent être spécifiées dans les critères de filtre peut être obtenue à l'aide de l'API /openapi/v1/inventory/ search/dimensions.

Paramètres :

Nom	Type	Description
filter	JSON	Une requête de filtre.
scopeName	chaîne	(Facultatif) Nom de la portée par laquelle les résultats doivent être limités.
limit	nombre entier	(facultatif) Nombre maximal de résultats à renvoyer.

Nom	Type	Description
offset	nombre entier	(facultatif) Décalage par rapport à la demande précédente pour obtenir la page suivante.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "filter": {
        "type": "contains",
        "field": "hostname",
        "value": "collector"
    },
    "scopeName": "Default:Production:Web",  // optional
    "limit": 100,
    "offset": "<offset-object>"               // optional
}
```

Pour connaître les différents types de filtres pris en charge, reportez-vous à Filtres, on page 1020

Le corps de la requête se compose d'un corps JSON avec les clés suivantes.

Clés	Valeurs
filtrer	Filtre de requête. Si le filtre est vide (c.-à-d. {}), la requête correspond à tous les éléments de l'inventaire.
scopeName	Nom complet de la portée à laquelle la requête est limitée (facultatif)
dimensions	Liste des noms de dimensions à renvoyer dans le résultat de l'API de recherche d'inventaire. Il s'agit d'un paramètre facultatif. S'il n'est pas spécifié, les résultats renvoient toutes les dimensions disponibles. Cette option est utile pour spécifier un sous-ensemble des dimensions disponibles lorsque l'appelant ne se soucie pas du reste des dimensions.
limit	Limite du nombre d'éléments de réponse (facultatif)
offset	Objet décalage reçu de la réponse précédente (facultatif)

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Nom	Type	Description
offset	nombre entier	Décalage de réponse à transmettre pour la page de résultats suivante.
results	tableau d'objets	Liste des résultats.

La réponse peut contenir un champ `décalage` pour les réponses paginées. Les utilisateurs devront spécifier le même décalage dans la demande suivante pour obtenir la prochaine série de résultats.

Exemple de code Python

```
req_payload = {
  "scopeName": "Tetration", # optional
  "limit": 2,
  "filter": {"type": "and",
     "filters": [
        {"type": "eq", "field": "vrf_name", "value": "Tetration"},
        {"type": "subnet", "field": "ip", "value": "1.1.1.0/24"},
        {"type": "contains", "field": "hostname", "value": "collector"}
     ]
  }
}

resp = restclient.post('/inventory/search', json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Statistiques d'inventaire

Ce point terminal renvoie des statistiques sur les éléments d'inventaire.

`GET /openapi/v1/inventory/{id}/stats?t0=<t0>&t1=<t1>&td=<td>`

Table 70:

Paramètres du chemin	Description
ID	ID de l'élément en d'inventaire comme `{ip}-{vrf_id}`, par exemple sur `1.1.1.1-123`

Paramètres de requête	Description
t0	Heure de début des statistiques en heure d'origine
t1	Heure de fin des statistiques en heure d'origine
td	Granularité pour les agrégations de statistiques. Un entier spécifie le nombre de secondes. Des chaînes peuvent être transmises, telles que « minute », « heure » et « jour ».

Exemple de code Python

```
resp = restclient.get('/inventory/1.1.1.1-123/stats?t0=1483228800&t1=1485907200&td=day')
```

Inventaire

Ce point terminal renvoie le nombre d'éléments de l'inventaire correspondant aux critères spécifiés.

```
POST /openapi/v1/inventory/count
```

La liste des colonnes qui peuvent être spécifiées dans les critères de filtre peut être obtenue à l'aide de l'API `/openapi/v1/inventory/ search/dimensions`.

Paramètres :

Nom	Type	Description
filter	JSON	Une requête de filtre.
scopeName	chaîne	(Facultatif) Nom de la portée par laquelle les résultats doivent être limités.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "filter": {
        "type": "and",
        "filters": [
            {
                "type": "contains",
                "field": "hostname",
                "value": "prod"
            },
            {
                "type": "subnet",
                "field": "ip"
                "value": "6.6.6.0/24"
            }
        ]
    },
    "scopeName": "Default:Production:Web",  # optional
}
```

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Table 71:

Clés	Valeurs
Nombre	Nombre d'éléments de l'inventaire correspondant aux critères du filtre

Exemple de code Python

```
req_payload = {
  "scopeName": "Tetration", # optional
  "filter": {"type": "and",
     "filters": [
        {"type": "eq", "field": "vrf_name", "value": "Tetration"},
        {"type": "subnet", "field": "ip", "value": "1.1.1.0/24"},
        {"type": "contains", "field": "hostname", "value": "collector"}
     ]
  }
```

```
}

resp = restclient.post('/inventory/count', json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Vulnérabilité de l'inventaire

Ce point terminal renvoie les CVE correspondant aux adresses IP associées aux charges de travail vulnérables.

Cette API est uniquement disponible pour les utilisateurs disposant au minimum d'un accès en lecture à la portée racine.

```
POST /openapi/v1/inventory/cves/{rootScopeID}
```

Paramètres :

Nom	Type	Description
ips	liste de chaînes	Liste des adresses IP pour récupérer les informations CVE.

Le corps de la demande doit être une requête au format JSON. Un exemple de corps de requête est présenté ci-dessous.

```
{
    "ips": [
        "10.18.187.72",
        "10.18.187.73"
    ]
}
```

Réponse

La réponse est un tableau d'objets JSON contenu dans le corps du message, avec les propriétés suivantes.

Nom	Type	Description
ip	chaîne	Adresse IP
cve_ids	liste de chaînes	Liste des ID CVE dans l'inventaire avec l'adresse IP.

Exemple de code Python

```
root_scope_id = "5fa0d242497d4f7d968c669b"
req_payload = {
  "ips":["10.18.187.72", "10.18.187.73"]
}

resp = restclient.post('/inventory/cves/' + root_scope_id,
json_body=json.dumps(req_payload))
print resp.status_code
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp, indent=4, sort_keys=True)
```

Charge de travail

L'API de la charge de travail fournit un accès programmatique au contenu de la page Profil de la charge de travail *(Profil de la charge de travail)*. Cet ensemble d'API nécessite la fonctionnalité `sensor_management` ou `flow_inventory_query` associées à la clé API.

Détails de la charge de travail

Ce point terminal renvoie la charge de travail spécifique étant donné une UUID de l'agent.

```
GET /openapi/v1/workload/{uuid}
```

Paramètres du chemin	Description
UUID	UUID de l'agent

Réponse

La réponse est un objet de charge de travail associé à l'UUID spécifié. Le schéma des attributs de l'objet de charge de travail est décrit ci-dessous :

Table 72:

Attribut	Type	Description
agent_type	nombre entier	Type d'agent dans l'énumération
agent_type_str	chaîne	Type d'agent en texte brut
auto_upgrade_opt_out	booléen	Si la valeur est « vrai », les agents ne sont pas mis à niveau automatiquement lors de la mise à niveau de la grappe.
cpu_quota_mode	nombre entier	Contrôle de quota du processeur
cpu_quota_us	nombre entier	Utilisation du processeur
current_sw_version	chaîne	Version du logiciel agent exécutée sur la charge de travail
data_plane_disabled	booléen	Si la valeur est « vrai », les données de télémétrie de flux ne sont pas exportées de l'agent vers la grappe
desired_sw_version	chaîne	La version du logiciel agent destinée à être exécutée sur la charge de travail
enable_conversation_flows	booléen	Si la valeur est True (vraie), le mode conversation est activé.

Attribut	Type	Description
enable_cache_sidechannel	booléen	Si la valeur est True (vraie), la détection des attaques par canal auxiliaire est activée
enable_forensics	booléen	Si la valeur est True (vraie), l'investigation criminalistique est activée
enable_meltdown	booléen	Si la valeur est True (vraie), la détection d'exploit de fusion est activée
enable_pid_lookup	booléen	Si la valeur est True (vraie), la recherche de processus est activée
forensics_cpu_quota_mode	nombre entier	Contrôle du quota du processeur pour la criminalistique
forensics_cpu_quota_us	nombre entier	Utilisation des quotas de criminalistique
criminalistique_mem_quota_octets	nombre entier	Quota de mémoire destiné à la criminalistique en octets
host_name	chaîne	Nom d'hôte sur la charge de travail
interfaces	tableau	Tableau d'objets Interface
kernel_version	chaîne	Version du noyau
last_config_fetch_at	nombre entier	Dernière configuration récupérée le
last_software_update_at	nombre entier	Horodatage auquel l'agent a signalé sa version actuelle.
max_rss_limit	nombre entier	Limite de mémoire maximale
intégrée	chaîne	Plateforme de la charge de travail
UUID	chaîne	Identifiant unique de l'agent
windows_enforcement_mode	chaîne	Type de mode d'application Windows, WAF (Windows Advanced Firewall, pare-feu avancé Windows) ou WFP (Windows Filtering Platform, plateforme de filtrage Windows)

Exemple de code Python

```
agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
resp = restclient.get('/workload/%s' % (agent_uuid))
```

Statistiques de la charge de travail

Ce point terminal renvoie des statistiques pour une charge de travail.

```
GET /openapi/v1/workload/{uuid}/stats?t0=<t0>&t1=<t1>&td=<td>
```

Paramètres du chemin	Description
UUID	UUID de l'agent

L'URL de la requête contient les paramètres suivants :

Paramètres de requête	Description
t0	Heure de début des statistiques en heure d'origine
t1	Heure de fin des statistiques en heure d'origine L'heure de fin ne peut pas dépasser l'heure de début de plus d'un jour.
td	Granularité pour les agrégations de statistiques. Un entier spécifie le nombre de secondes. Des chaînes peuvent être transmises, telles que « minute », « heure » et « jour ».

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Nom	Type	Description
Horodatage	chaîne	Heure à laquelle les mesures ont été recueillies (heure d'origine ou ISO 8601)
results	objet	Indicateurs

Les mesures sont un objet JSON avec les propriétés suivantes :

Nom	Type	Description
flow_count	nombre entier	Nombre de flux.
rx_byte_count	nombre entier	Le nombre d'octets reçus.
rx_packet_count	nombre entier	Nombre de paquets reçus
tx_byte_count	nombre entier	Nombre d'octets transmis.
tx_packet_count	nombre entier	Nombre de paquets transmis.

Exemple de code Python

```
 agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
 td = 15 * 60 # 15 minutes
 resp = restclient.get('/workload/%s/stats?t0=1483228800&t1=1485907200&td=%d' % (agent_uuid,
td))

 # This code queries workload statistics for a week
 t0 = 1483228800
 for _ in range(7):
   t1 = t0 + 24 * 60 * 60
   resp = restclient.get('/workload/%s/stats?t0=%d&t1=%d&td=day' % (agent_uuid, t0, t1))
   t0 = t1
```

Paquets logiciels installés

Ce point terminal renvoie la liste des paquets logiciels installés sur le charges de travail.

```
GET /openapi/v1/workload/{uuid}/packages
```

Paramètres du chemin	Description
UUID	UUID de l'agent

Réponse

La réponse est un tableau d'objets JSON paquets logiciels. Le schéma de l'objet paquet est décrit ci-dessous :

Attribut	Type	Description
architecture	chaîne	Architecture du paquet
name	chaîne	Nom du paquet
publisher	chaîne	Serveur de publication du paquet
version	chaîne	Version du paquet

Exemple de code Python

```
 agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
 resp = restclient.get('/workload/%s/packages' % (agent_uuid))
```

Vulnérabilités de la charge de travail

Ce point terminal renvoie la liste des vulnérabilités observées sur la charge de travail.

```
GET /openapi/v1/workload/{uuid}/vulnerabilities
```

L'objet de vulnérabilités se compose d'un corps JSON avec les clés suivantes.

Paramètres du chemin	Description
UUID	UUID de l'agent

Réponse

La réponse est un tableau d'objets JSON de vulnérabilité. Le schéma de l'objet de vulnérabilité est décrit ci-dessous :

Attribut	Type	Description
cve_id	chaîne	ID d'exposition à la vulnérabilité commune
package_infos	tableau	Tableau d'objets Renseignements sur le paquet
v2_score	flottant	Note CVSS V2
v2_access_complexity	chaîne	Complexité d'accès CVSS V2
v2_access_vector	chaîne	vecteur d'accès CVSS V2
v2_authentication	chaîne	Authentification CVSS V2
v2_availability_impact	chaîne	Incidence sur la disponibilité de CVSS V2
v2_confidentiality_impact	chaîne	Incidence sur la confidentialité de CVSS V2
v2_integrity_impact	chaîne	Incidence sur l'intégrité de CVSS V2
v2_severity	chaîne	Gravité de CVSS V2
v3_score	flottant	Note CVSS V3
v3_attack_complexity	chaîne	Complexité des attaques CVSS V3
v3_attack_vector	chaîne	Vecteur d'attaque CVSS V3
v3_availability_impact	chaîne	Incidence sur la disponibilité de CVSS V3
v3_base_severity	chaîne	Gravité de base CVSS V3
v3_confidentiality_impact	chaîne	Incidence sur la confidentialité de CVSS V2
v3_integrity_impact	chaîne	Incidence sur l'intégrité de CVSS V3
v3_privileges_required	chaîne	Privilèges CVSS V3 requis
v3_scope	chaîne	Portée de CVSS V3
v3_user_interaction	chaîne	Interaction avec l'utilisateur CVSS V3

Exemple de code Python

```
agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
resp = restclient.get('/workload/%s/vulnerabilities' % (agent_uuid))
```

Processus de longue durée de la charge de travail

Ce point terminal renvoie la liste des processus de longue durée sur la charge de travail. Les processus de longue durée sont définis comme des processus qui ont un temps de disponibilité d'au moins 5 minutes.

```
GET /openapi/v1/workload/{uuid}/process/list
```

Paramètres du chemin	Description
UUID	UUID de l'agent

Réponse

La réponse est une liste de processus d'objets JSON.

Attribut	Type	Description
CMD	chaîne	Chaîne de commande du processus
binary_hash	chaîne	SHA256 du binaire de processus en hexadécimal
ctime	long	ctime du processus binaire en nous
mtime	long	mtime du processus binaire en nous
exec_path	chaîne	Chemin d'accès de l'exécutable du processus
exit_usec	long	Heure de sortie du processus
num_libs	nombre entier	Nombre de bibliothèques chargées par le processus
pid	nombre entier	Identifiant de processus
ppid	nombre entier	ID du processus parent
pkg_info_name	chaîne	Nom du paquet associé au processus
pkg_info_version	chaîne	Version du paquet associé au processus
proc_state	chaîne	État du processus
disponibilité	long	Disponibilité du processus en nous
username	chaîne	Nom d'utilisateur du processus

Attribut	Type	Description
resource_usage	tableau objet	Tableau d' Utilisation des ressources

Exemple de code Python

```
agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
resp = restclient.get('/openapi/v1/workload/%s/process/list' % (agent_uuid))
```

Résumé de l'instantané du processus de charge de travail

Ce point terminal renvoie un résumé d'instantané de processus pour cette charge de travail. Un instantané de processus contient tous les processus capturés par la charge de travail à un moment donné. Actuellement, une copie du dernier instantané de processus est conservée. Le point terminal prend en charge la méthode POST avec une charge utile vide pour faciliter une extension future.

```
POST /openapi/v1/workload/{uuid}/process/tree/ids
```

Paramètres du chemin	Description
UUID	UUID de l'agent

Réponse

La réponse est une liste d'objets JSON récapitulatifs d'instantané de processus.

Attribut	Type	Description
sensor_uuid	chaîne	UUID de l'agent
handle	chaîne	Descripteur de l'instantané de processus à récupérer
process_count	nombre entier	Nombre de processus dans l'instantané
ts_usec	nombre entier	Horodatage de capture de l'instantané

Exemple de code Python

```
agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
payload = {
}
resp = restclient.post('/openapi/v1/workload/%s/process/tree/ids' %
                       agent_uuid, json_body=json.dumps(payload))
```

Instantané du processus de charge de travail

Ce point terminal renvoie un instantané de processus sur cette charge de travail. Un instantané de processus contient tous les processus capturés par la charge de travail à un moment donné. Actuellement, une copie du

dernier instantané de processus est conservée. Ce point terminal doit être utilisé avec le point de terminaison de résumé d'instantané du processus de charge de travail.

```
POST /openapi/v1/workload/{uuid}/process/tree/details
```

Paramètres du chemin	Description
UUID	UUID de l'agent

Champ de charge utile	Type	Description
handle	chaîne	Descripteur de l'instantané de processus à récupérer

Réponse

La réponse est une liste de processus appartenant à l'instantané en JSON.

Attribut	Type	Description
command_string	chaîne	Chaîne de commande marquée d'un jeton
command_string_raw	chaîne	Chaîne de commande brute
binary_hash	chaîne	SHA256 du binaire de processus en hexadécimal
ctime	long	ctime du processus binaire en nous
mtime	long	mtime du processus binaire en nous
exec_path	chaîne	Chemin d'accès de l'exécutable du processus
Process-id	nombre entier	Identifiant de processus
parent_process_id	nombre entier	ID du processus parent
process_key	nombre entier	Clé unique du processus
parent_process_key	nombre entier	Clé unique pour le processus parent
pkg_info_name	chaîne	Nom du paquet associé au processus
pkg_info_version	chaîne	Version du paquet associé au processus
proc_state	chaîne	État du processus
disponibilité	long	Disponibilité du processus en nous
username	chaîne	Nom d'utilisateur du processus
cve_ids	tableau	Tableau d'objets CVEID

Exemple de code Python

```
agent_uuid = 'aa28b304f5c79b2f22d87a5af936f4a8fa555894'
payload = {
}
resp = restclient.post('/openapi/v1/workload/%s/process/tree/ids' %
            agent_uuid, json_body=json.dumps(payload))
handle = json.loads(resp.text)['process_summary'][0]['summary'][0]['handle']
payload = {
  "handle": handle,
}
resp = restclient.post('/openapi/v1/workload/%s/process/tree/details' %
            agent_uuid, json_body=json.dumps(payload))
```

Définitions d'objets JSON

Interface

Attribut	Type	Description
ip	chaîne	L'adresse IP de l'interface.
MAC	chaîne	L'adresse MAC de l'interface.
name	chaîne	Le nom de l'interface:
masque réseau	chaîne	Masque réseau de l'interface
pcap_opened	booléen	Si la valeur est False, les captures de paquets ne sont pas activées pour l'interface
tags_scope_id	tableau	ID de la portée associés à l'interface
VRF	chaîne	Nom VRF
vrf_id	nombre entier	ID VRF

Renseignements sur le paquet

Attribut	Type	Description
name	chaîne	Nom du paquet
version	chaîne	Version du paquet

Utilisation des ressources

Attribut	Type	Description
cpu_usage	flottant	Utilisation du processeur

Attribut	Type	Description
memory_usage_kb	nombre entier	Utilisation de la mémoire
ts_usec	long	Horodatage de l'heure à laquelle l'utilisation de la ressource a été capturée.

ID CVE

Attribut	Type	Description
cve_id	chaîne	ID CVE
impact__cvss_v2__access_complexity	chaîne	complexité de l'accès CVE
impact__cvss_v2__access_vector	chaîne	vecteur d'accès CVE

Configuration de génération de politiques par défaut

Cet ensemble d'API est utilisé pour lire et mettre à jour la configuration de génération de politiques par défaut pour une portée racine.

Les API nécessitent la capacité `app_policy_management` associée à la clé API.

Remarque Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

- Objet configuration de génération de politiques, à la page 1039
- Obtenir la configuration de génération de politiques par défaut, à la page 1041
- Définir la configuration de génération de politiques par défaut, à la page 1041

Objet configuration de génération de politiques

Attribut	Type	Description
carry_over_policies	booléen	Toute politique marquée comme approuvée sera maintenue, si possible
deep_policy_generation	booléen	crée des politiques pour l'ensemble de l'arborescence de la portée sous la portée donnée, y compris tous les membres de la portée donnée

Attribut	Type	Description
skip_clustering	booléen	défini à vrai pour ignorer la mise en grappe, génère des politiques avec des grappes et des portées approuvées existantes
auto_accept_policy_connectors	booléen	accepte automatiquement tous les connecteurs de politique sortants
enable_exclusion_filter	booléen	appliquer des filtres d'exclusion aux données de flux d'entrée
enable_default_exclusion_filter	booléen	appliquer des filtres d'exclusion par défaut aux données de flux d'entrée
remove_redundant_policies	booléen	supprimer les politiques redondantes lors de la génération approfondie des politiques
enable_service_discovery	booléen	le paramètre faux permet d'ignorer la génération de politiques basées sur la plage de ports éphémères dans le pipeline adm rapporté par le capteur, actuellement utilisé pour générer des politiques pour Windows Active Directory.
externals	tableau	liste ordonnée des objets de dépendance externes
clustering_granularity	chaîne	un choix parmi VERY_COARSE (TRÈS GROSSIÈRE), COARSE (GROSSIÈRE), MEDUM (MOYENNE), FINE (FINE), VERY_FINE (TRÈS FINE)
policy_compression	chaîne	un choix parmi : DISABLED (DÉSACTIVÉE), CONSERVATIVE (CONSERVATRICE), MODERATE (MODÉRÉE), AGRESSIVE (AGRESSIVE), VERY_AGGRESSIVE (TRÈS AGRESSIVE)
port_generalization	chaîne	un choix parmi : DISABLED (DÉSACTIVÉE), CONSERVATIVE (CONSERVATRICE), MODERATE (MODÉRÉE), AGRESSIVE (AGRESSIVE), VERY_AGGRESSIVE (TRÈS AGRESSIVE)
sim_policy	nombre entier	1 => flux, 2 => processus, 5 => les deux

L'objet de dépendance externe

Nom	Type	Description
ID	chaîne	ID du filtre
filter_type	chaîne	AppScope ou UserInventoryFilter
inclure	tableau	objet avec user_filters booléen pour activer et user_filter_list pour la liste ordonnée des filtres d'inventaire de service fournis

Obtenir la configuration de génération de politiques par défaut

Ce point terminal renvoie la configuration par défaut actuelle de la génération de politiques. Peut renvoyer un objet vide si aucun objet n'a été créé.

```
GET /openapi/v1/app_scopes/default_adm_run_config
```

Paramètres :

L'URL de la demande contient les paramètres suivants

Nom	Type	Description
root_app_scope_id	chaîne	Identificateur unique de la portée racine à laquelle cette configuration par défaut s'applique

Objet de réponse : renvoie la configuration de génération de politique par défaut actuelle ou un objet vide si aucune configuration n'a été créée.

Définir la configuration de génération de politiques par défaut

Ce point terminal définit la configuration de génération de politiques par défaut

```
PUT /openapi/v1/app_scopes/default_adm_run_config
```

Paramètres en plus des valeurs de la liste d'objets de configuration de génération de politique ci-dessus.

Nom	Type	Description
root_app_scope_id	chaîne	Identificateur unique de la portée racine à laquelle cette configuration par défaut s'applique

Objet de la réponse : renvoie la configuration de génération de politiques par défaut.

Intent criminalistique

Les API des agents logiciels sont associées à la gestion des intents criminalistiques.

Les intents criminalistiques lient un profil criminalistique au groupe d'agents auquel il s'applique. Le groupe d'agents est défini à l'aide d'un filtre d'inventaire.

Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API.

Remarque Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

Objet intent criminalistique

Attribut	Type	Description
ID	chaîne	identifiant unique de l'intent
name	chaîne	nom de l'intent
inventory_filter_id	tableau	ID du filtre d'inventaire associé à l'intent
forensic_config_profile_id	nombre entier	ID du profil associé à cet intent
created_at	nombre entier	Horodatage Unix de la création de l'intent
updated_at	nombre entier	Horodatage Unix de la dernière mise à jour de l'intent

Liste des intents criminalistiques

Ce point terminal répertorie tous les profils criminalistiques existants

```
GET /openapi/v1/inventory_config/forensic_intents
```

Paramètres : Aucun

Ce point terminal renvoie un tableau de résumés d'objets intents criminalistiques

Récupération d'un intent criminalistique unique

```
GET /openapi/v1/inventory_config/forensic_intents/{intent_id}
```

Paramètres :

Nom	Type	Description
intent_id	chaîne	ID de l'intent

Renvoie une représentation détaillée de l'objet intent criminalistique.

Création d'un intent criminalistique

```
POST /openapi/v1/inventory_config/forensic_intents
```

Paramètres :

Nom	Type	Description
name	chaîne	nom de l’intent
inventory_filter_id	chaîne	ID du filtre d’inventaire associé à l’intent
forensic_config_profile_id	chaîne	ID du profil criminalistique associé à l’intent

Renvoie un objet intent criminalistique.

Mettre à jour un intent criminalistique

```
PUT /openapi/v1/inventory_config/forensic_intents/{intent_id}
```

Paramètres :

Nom	Type	Description
intent_id	chaîne	ID de l’intent
name	chaîne	nom de l’intent
inventory_filter_id	chaîne	ID du filtre d’inventaire associé à l’intent
forensic_config_profile_id	chaîne	ID du profil criminalistique associé à l’intent

Renvoie un objet intent criminalistique.

Supprimer un intent criminalistique

```
DELETE /openapi/v1/inventory_config/forensic_intents/{intent_id}
```

Paramètres :

Nom	Type	Description
intent_id	chaîne	ID de l’intent

Retourne 200 en cas de réussite.

Ordres des intents criminalistiques

Les API des agents logiciels sont associées à la gestion de l'ordre des intents criminalistiques.

Les profils criminalistiques sont appliqués aux agents à l'aide d'intents. Les intents utilisent des filtres d'inventaire pour définir les groupes d'agents. Si les filtres se chevauchent, nous devons savoir lesquels appliquer. Nous utilisons un ordre pour définir la priorité des intents.

Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API.

Remarque Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

- Objet ordre d'intent criminalistique, à la page 1044
- Récupérer l'ordre actuel des intents criminalistiques, à la page 1044
- Création d'un intent criminalistique, à la page 1043

Objet ordre d'intent criminalistique

Attribut	Type	Description
version	chaîne	version de l'ordre actuel
intents	tableau	nom des objets d'intent dans l'ordre
intent_ids	tableau	tableau d'ID d'intents criminalistiques

Récupérer l'ordre actuel des intents criminalistiques

Ce point terminal renvoie l'ordre actuel des intents criminalistiques.

```
GET /openapi/v1/inventory_config/forensic_orders
```

Paramètres : Aucun

Ce point terminal renvoie l'objet ordre actuel des intents criminalistiques.

Création d'un ordre d'intent criminalistique

```
POST /openapi/v1/inventory_config/forensic_orders
```

Paramètres :

Nom	Type	Description
version	chaîne	doit correspondre à la commande en cours

Nom	Type	Description
intent_ids	tableau	tableau d'ID d'intent

Renvoie un objet ordre d'intent criminalistique.

Profils criminalistiques

Les API des agents logiciels sont associées à la gestion des profils criminalistiques.

Les profils criminalistiques sont des ensembles de règles qui peuvent être appliquées aux groupes d'agents utilisant les intents criminalistiques.

Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API.

Remarque Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

Objet profil criminalistique

Attribut	Type	Description
ID	chaîne	identifiant unique du profil
name	chaîne	nom du profil
forensic_rules	tableau	tableau des règles associées au profil
created_at	nombre entier	Horodatage Unix de la création du profil
updated_at	nombre entier	Horodatage Unix de la dernière mise à jour du profil
is_readonly	booléen	indique si le profil est en lecture seule
root_app_scope_id	chaîne	ID de la portée racine à laquelle le profil appartient

Répertorier les profils criminalistiques

Ce point terminal répertorie tous les profils criminalistiques existants

```
GET /openapi/v1/inventory_config/forensic_profiles
```

Paramètres : Aucun

Ce point terminal renvoie un tableau de résumés d'objets profils criminalistiques.

Récupération d'un seul profil criminalistique

```
GET /openapi/v1/inventory_config/forensic_profiles/{profile_id}
```

Paramètres :

Nom	Type	Description
profile_id	chaîne	ID du profil

Renvoie une représentation détaillée de l'objet profil criminalistique.

Création d'un profil criminalistique

```
POST /openapi/v1/inventory_config/forensic_profiles
```

Paramètres :

Nom	Type	Description
name	chaîne	nom du profil
root_app_scope_id	chaîne	ID de la portée racine à laquelle le profil appartient
forensic_rule_ids	tableau	Tableau d'ID de règles criminalistiques à associer à ce profil

Renvoie un objet de profil criminalistique.

Mettre à jour un profil criminalistique

```
PUT /openapi/v1/inventory_config/forensic_profiles/{id}
```

Paramètres :

Nom	Type	Description
profile_id	chaîne	ID du profil
name	chaîne	nom du profil

Nom	Type	Description
forensic_rule_ids	tableau	Tableau d'ID de règles criminalistiques à associer à ce profil

Renvoie un objet de profil criminalistique.

Supprimer un profil criminalistique

```
DELETE /openapi/v1/inventory_config/forensic_profiles/{profile_id}
```

Paramètres :

Nom	Type	Description
profile_id	chaîne	ID du profil

Retourne 200 en cas de réussite.

Règles criminalistiques

Les API des agents logiciels sont associées à la gestion des règles criminalistiques.

Les règles criminalistiques sont utilisées dans les profils criminalistiques qui sont ensuite appliqués à des groupes d'agents.

Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API.

Remarque Ces API ne sont disponibles que pour les administrateurs de site et les propriétaires de portées racine.

- Objet règle criminalistique, à la page 1047
- Liste des règles criminalistiques, à la page 1048
- Récupération d'une seule règle criminalistique, à la page 1048
- Création d'une règle criminalistique, à la page 1049
- Mettre à jour une règle criminalistique, à la page 1049
- Supprimer une règle criminalistique, à la page 1050

Objet règle criminalistique

Attribut	Type	Description
ID	chaîne	identifiant unique de la règle
name	chaîne	nom de la règle

Attribut	Type	Description
description	chaîne	description de la règle
type	chaîne	PREDEFINED (PRÉDÉFINI) ou USER_DEFINED (UTILISATEUR DÉFINI)
eval_group_type	chaîne	AS_INDIVIDUAL (COMME_INDIVIDU) ou AS_GROUP (COMME_GROUPE)
gravité	chaîne	l'un des éléments suivants : IMMEDIATE_ACTION, CRITICAL, HIGH, MEDIUM, LOW (ACTION_IMMÉDIATE, CRITIQUE, ÉLEVÉE, MOYENNE ou FAIBLE)
Actions	tableau	Tableau ou chaînes ALERT (ALERTE) ou REPORT (RAPPORT)
created_at	nombre entier	Horodatage Unix de la création de la règle
updated_at	nombre entier	Horodatage Unix de la dernière mise à jour de la règle

Liste des règles criminalistiques

Ce point terminal répertorie toutes les règles criminalistiques existantes

```
GET /openapi/v1/inventory_config/forensic_rules
```

Paramètres : Aucun

Ce point terminal renvoie un tableau de résumés d'objets de règles criminalistiques.

Récupération d'une seule règle criminalistique

```
GET /openapi/v1/inventory_config/forensic_rules/{rule_id}
```

Paramètres :

Nom	Type	Description
rule_id	chaîne	ID de la règle

Renvoie une représentation détaillée de l'objet règle criminalistique.

Création d'une règle criminalistique

```
POST /openapi/v1/inventory_config/forensic_rules
```

Paramètres :

Nom	Type	Description
root_app_scope_id	chaîne	ID de la portée racine à laquelle cette règle appartient
name	chaîne	nom de la règle
description	chaîne	description de la règle
eval_group_type	chaîne	type de règle
gravité	chaîne	gravité de la règle
Actions	tableau	Tableau ou chaînes ALERT (ALERTE) ou REPORT (RAPPORT)
clause	chaîne	la clause de la requête de la règle.

Renvoie un objet de règle criminalistique.

Mettre à jour une règle criminalistique

```
PUT /openapi/v1/inventory_config/forensic_rules/{rule_id}
```

Paramètres :

Nom	Type	Description
rule_id	chaîne	ID de la règle
name	chaîne	nom de la règle
description	chaîne	description de la règle
eval_group_type	chaîne	type de règle
gravité	chaîne	gravité de la règle
Actions	tableau	Tableau ou chaînes ALERT (ALERTE) ou REPORT (RAPPORT)
clause	chaîne	la clause de la requête de la règle.

Renvoie un objet de règle criminalistique.

Supprimer une règle criminalistique

```
DELETE /openapi/v1/inventory_config/forensic_rules/{rule_id}
```

Paramètres :

Nom	Type	Description
rule_id	chaîne	ID de la règle

Retourne 200 en cas de réussite.

Paramètres de la plateforme

Cet ensemble d'API peut être utilisé pour ajouter, modifier ou supprimer des paramètres de plateforme et nécessite la fonctionnalité appliance_management associée à la clé API.

Note Ces API sont uniquement disponibles pour le service d'assistance à la clientèle et les administrateurs de site.

Obtenir des certificats

Ce point terminal est utilisé pour récupérer les certificats SSL/TLS.

```
GET /openapi/v1/platform_settings/outbound_http
```

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
nom_paire_clés	chaîne	Précisez le nom de la paire de clés.
cert_sha1	chaîne	L'identifiant unique du certificat.
created_at	chaîne	Récupérer les certificats créés à partir d'une date et d'une heure précises.

Obtenir les paramètres d'analyse de l'utilisation

Ce point terminal est utilisé pour récupérer les paramètres liés à l'analyse de l'utilisation ou à la collecte de données de télémétrie dans la plateforme.

```
GET /openapi/v1/platform_settings/ usage_analytics
```

Paramètres :

Nom	Type	Description
query	objet	Récupérer les paramètres liés à l'analyse de l'utilisation ou à la collecte de données de télémétrie.

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
usage_analytics_enabled	booléen	Indiquer si l'analyse de l'utilisation ou la collecte de données de télémétrie est activée ou désactivée.

Obtenir les message de connexion

Ce point terminal est utilisé pour récupérer le message de connexion personnalisé qui s'affiche pour les utilisateurs sur la plateforme.

```
GET /openapi/v1/platfor_settings/ login_message
```

Il n'y a aucun paramètre pour le point terminal get log message (récupération du message de connexion).

Obtenir les paramètres HTTP sortants

Ce point terminal est utilisé pour récupérer les paramètres HTTP sortants actuels configurés pour la plateforme.

```
GET /openapi/v1/platform_settings/outbound_http
```

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
outbound_http_enabled	chaîne	Indiquer si les connexions HTTP sortantes sont activées.

Mettre à jour les paramètres HTTP sortants

Ce point terminal est utilisé pour récupérer les paramètres HTTP sortants actuels configurés pour la plateforme.

```
POST /openapi/v1/ platform_settings/ outbound_http
```

Paramètres :

Nom	Type	Description
query	objet	Mettez à jour les paramètres HTTP sortants configurés pour la plateforme.

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
`outbound_http_enabled`	chaîne	Indiquer si les connexions HTTP sortantes sont activées.

Tester les paramètres HTTP sortants

Ce point terminal est utilisé pour tester les paramètres HTTP sortants actuellement configurés pour la plateforme.

```
POST openapi/v1/platform_settings/outbound_http_test
```

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
`opération réussie`	booléen	Vérifiez si la connexion HTTP sortante est réussie.

Obtenir les paramètres de serveur mandataire HTTP sortants

Ce point terminal est utilisé pour récupérer les paramètres du serveur mandataire HTTP sortants configurés pour la plateforme.

```
GET /openapi/v1/platform_settings/outbound_http_proxy
```

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
outbound_http_enabled	booléen	Indiquez si la connexion HTTP sortante est activée.
http_proxy_enabled	booléen	Indiquer si un serveur mandataire HTTP est activé.
http_proxy_server	chaîne	Récupérer le serveur mandataire HTTP sortant configuré.
http_proxy_port	nombre entier	Précisez le numéro de port utilisé pour le serveur mandataire HTTP.
http_proxy_username	chaîne	Précisez le nom d'utilisateur utilisé pour l'authentification auprès du serveur mandataire HTTP.
http_proxy_password_present	booléen	Déterminez si la plateforme est actuellement configurée pour utiliser un mot de passe pour l'authentification auprès du serveur mandataire HTTP.

Mettre à jour les paramètres de serveur mandataire HTTP sortant

Ce point terminal est utilisé pour récupérer les paramètres du serveur mandataire HTTP sortants configurés pour la plateforme.

```
POST /openapi/v1/ platform_settings/ outbound_http_proxy
```

La réponse est un objet JSON comportant le schéma suivant :

Clé	Type	Valeur
outbound_http_enabled	booléen	Indiquez si la connexion HTTP sortante est activée.
http_proxy_enabled	booléen	Indiquer si un serveur mandataire HTTP est activé.
http_proxy_server	chaîne	Récupérer le serveur mandataire HTTP sortant configuré.
http_proxy_port	nombre entier	Précisez le numéro de port utilisé pour le serveur mandataire HTTP.
http_proxy_username	chaîne	Précisez le nom d'utilisateur utilisé pour l'authentification auprès du serveur mandataire HTTP.
http_proxy_password_present	booléen	Déterminez si le mot de passe est disponible.

Exécution

L'application des politiques est la fonctionnalité par laquelle les politiques générées sont envoyées vers les ressources de la portée associée à un espace de travail et de nouvelles règles de pare-feu sont écrites. Cet ensemble d'API nécessite la capacité `app_policy_management` associée à la clé API.

Pour en savoir plus, consultez la section Appliquer des politiques.

Configuration de politique de réseau de l'agent

Ce point terminal renvoie un objet Agent en fonction de l'ID d'agent. Ceci est utile pour récupérer la politique de réseau, la configuration de l'agent, sa version, etc.

```
GET /openapi/v1/enforcement/agents/{aid}/network_policy_config
```

Paramètres :

L'URL de la demande contient les paramètres suivants

Nom	Type	Description
aid	chaîne	UUID de l'agent pour la configuration de la politique de réseau

Le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
include_filter_names	booléen	Inclut les noms et les ID de filtres dans les politiques de réseau.
inject_versions	booléen	Inclut les versions des espaces de travail ADM dans les politiques de réseau.

Réponse

La réponse de ce point terminal est un objet Agent .

Statistiques sur la politique concrète

Ce point terminal renvoie les statistiques pour les politiques concrètes en fonction de l'ID d'agent et de l'ID de politique concrète. Le point terminal renvoie un tableau d'objets Série chronologique du résultat de la politique concrète.

```
GET /openapi/v1/enforcement/agents/{aid}/concrete_policies/{cid}/stats?t0=<t0>&t1=<t1>
↪&td=<td>
```

Paramètres :

L'URL de la demande contient les paramètres suivants

Nom	Type	Description
aid	chaîne	UUID de l'agent pour les statistiques.
cid	chaîne	Identifiant unique UUID de politique concrète pour les statistiques.

Le corps de la requête JSON contient les clés suivantes :

Table 73:

Nom	Type	Description
t0	nombre entier	Heure de début des statistiques en heure d'origine
t1	nombre entier	Heure de fin des statistiques en heure d'origine

Nom	Type	Description
td	nombre entier ou chaîne	Granularité pour les agrégations de statistiques. Un entier spécifie le nombre de secondes. Des chaînes peuvent être transmises, telles que « minute », « heure » et « jour ».

Définitions d'objets JSON

Agent

Attribut	Type	Description
agent_uuid	chaîne	UUID de l'agent.
agent_config	objet	Configuration de l'agent
agent_config_status	objet	État de configuration de l'agent
desired_network_policy_config	objet	Configuration de la politique de réseau
provisioned_network_policy_config	objet	Configuration de politique de réseau mise en service
provisioned_state_update_timestamp	nombre entier	horodatage d'origine en secondes de la prise en compte par l'agent de la politique mise en œuvre ci-dessus.
desired_policy_update_timestamp	nombre entier	horodatage d'origine en secondes de la génération de desired_network_policy_config.
agent_info	objet	Renseignements sur l'agent
skipped	booléen	Vrai (vrai) lorsque la génération de règles concrètes est ignorée.
message	chaîne	Raison pour laquelle la génération de politiques concrètes est ignorée

Configuration de l'agent

Attribut	Type	Description
agent_uuid	chaîne	UUID de l'agent.
enforcement_enabled	booléen	La configuration indiquant que l'application est activée sur l'agent.

Attribut	Type	Description
fail_mode	chaîne	Mode échec.
version	number	Numéro de version de la configuration de l'agent.
control_tet_rules_only	booléen	Configuration des règles de contrôle seulement
allow_broadcast	booléen	Autoriser la configuration de diffusion
allow_multicast	booléen	Autoriser la configuration de multidiffusion
allow_link_local	booléen	Autoriser le lien Configuration locale.
forcement_cpu_quota_mode	chaîne	Mode de quota de CPU de l'agent d'application.
enforcement_cpu_quota_us	chaîne	Quota de CPU de l'agent d'application en micro-secondes.
forcement_max_rss_limit	number	Limite RSS max. d'agents d'application

Configuration de la politique de réseau

Attribut	Type	Description
version	chaîne	Numéro de version
network_policy	tableau	Tableau d'objets de la Politique réseau
address_sets	tableau	Tableau d'objets Ensemble d'adresses pour la fonction d'ensemble IP.
container_network_policy	tableau	Tableau d'objets ContainerNetworkPolicy

Politique réseau

Attribut	Type	Description
priority	chaîne	Priorité d'une politique concrète
enforcement_intent_id	chaîne	ID d'intent d'application.
concrete_policy_id	chaîne	Identifiant de politique concrète

Attribut	Type	Description
match	objet	Mettre en correspondance des critères de la politique Ce champ est obsolète.
action	objet	Action pour la correspondance de politique.
workspace_id	chaîne	ID de l'espace de travail.
adm_data_set_id	chaîne	ID de l'ensemble de données de découverte automatique des politiques de l'espace de travail
adm_data_set_version	chaîne	la version de l'ensemble de données de découverte automatique des politiques de l'espace de travail. Défini uniquement lorsque inject_versions=vrai est transmis dans les paramètres
cluster_edge_id	chaîne	ID de périphérie de la grappe.
policy_intent_group_id	chaîne	ID de groupe d'intents de politique
match_set	objet	Objet d'Ensemble de correspondances pour la prise en charge d'ensembles IP. Un nombre exact de match ou match_set.
src_filter_id	chaîne	ID du filtre d'inventaire source Celui-ci sera défini lorsque la commande include_filter_names=vrai sera transmise en tant que paramètre.
src_filter_name	chaîne	Nom du filtre d'inventaire source. Celui-ci sera défini lorsque la commande include_filter_names=vrai sera transmise en tant que paramètre.
dst_filter_id	chaîne	ID du filtre d'inventaire de destination. Celui-ci sera défini lorsque la commande include_filter_names=vrai sera transmise en tant que paramètre.

Attribut	Type	Description
dst_filter_name	chaîne	Nom du filtre d'inventaire de destination. Celui-ci sera défini lorsque la commande include_filter_names=vrai sera transmise en tant que paramètre.

ContainerNetworkPolicy

Attribut	Type	Description
pod_id	chaîne	ID de POD.
network_policy	tableau	Tableau d'objets de la Politique réseau
déploiement	chaîne	Nom du déploiement
service_endpoint	tableau	Liste des noms de points terminaux de service.

Mettre en correspondance

Attribut	Type	Description
src_addr	objet	Objet de sous-Sous-réseau pour l'adresse source
dst_addr	objet	Objet de sous-Sous-réseau pour l'adresse de destination
src_port_range_start	int	Début de la plage du port source
src_port_range_end	int	Fin de la plage du port source
dst_port_range_start	int	Début de la plage du port de destination
dst_port_range_end	int	Fin de la plage du port de destination
ip_protocol	chaîne	Protocole IP
address_family	chaîne	Famille d'adresses IPv4 ou IPv6
direction	chaîne	Direction de la correspondance, INGRESS (ENTRÉE) ou EGRESS (SORTIE).
src_addr_range	objet	ObjetPlage d'adresses pour l'adresse source.

Attribut	Type	Description
dst_add_range	objet	ObjetPlage d'adresses pour l'adresse de destination.

Action

Attribut	Type	Description
type	chaîne	Type d'action

Ensemble de correspondances

Attribut	Type	Description
src_set_id	chaîne	ID d'ensemble source de l'objet de Ensemble d'adresses dans Configuration de la politique de réseau `Ensembles_d'adresses` tableau
dst_set_id	chaîne	Tableau des ID d'ensemble de destination de l'objet de Ensemble d'adresses dans Configuration de la politique de réseau `Ensembles_d'adresses`
src_ports	tab-leau	Tableau d'objets de Plage de ports pour les ports sources
dst_ports	tab-leau	Tableau d'objets de Plage de ports pour les ports de destination.
ip_protocol	chaîne	Protocole IP
address_family	chaîne	Famille d'adresses IPv4 ou IPv6
direction	chaîne	Direction de la correspondance, INGRESS (ENTRÉE) ou EGRESS (SORTIE).

Ensemble d'adresses

Attribut	Type	Description
id_ensemble	chaîne	ID d'ensemble d'adresses
addr_ranges	tableau	Tableau d'objets de Plage d'adresses

Attribut	Type	Description
subnets	tableau	Tableau d'objets deSous-réseau.
addr_family	chaîne	Famille d'adresses IPv4 ou IPv6

Sous-réseau

Attribut	Type	Description
ip_addr	chaîne	Adresse IP.
prefix_length	int	Longueur de préfixe pour le sous-réseau.

Plage d'adresses

Attribut	Type	Description
start_ip_addr	chaîne	Adresse IP de début de la plage
end_ip_addr	chaîne	Adresse IP de fin de la plage

Plage de ports

Attribut	Type	Description
start_port	int	Port de début de la plage.
end_port	int	Port de fin de la plage.

État de configuration de l'agent

Attribut	Type	Description
désactivé	booléen	La configuration indiquant que l'application est désactivée pour l'agent.
current_version	number	Version de configuration actuelle de l'agent appliquée à l'agent.
highest_seen_version	number	Version la plus récente de la configuration de l'agent reçue par l'agent.

Configuration de politique de réseau mise en service

Attribut	Type	Description
version	chaîne	Version de configuration de politique de réseau mise ne œuvre par l'agent.
error_reason	chaîne	CONFIG_SUCCESS (CONFIGURATION_SUCCÈS) lorsque l'agent a appliqué les politiques avec succès, sinon motif de l'erreur.
désactivé	booléen	La configuration indiquant que l'application est désactivée pour l'agent.
current_version	number	Version actuelle du NPC appliquée à l'agent.
highest_seen_version	number	Version la plus récente du NPC reçue par l'agent.
policy_status	objet	Chaque état de politique de réseau

Renseignements sur l'agent

Attribut	Type	Description
agent_info_supported	booléen	La capacité de l'agent si agent_info est pris en charge.
ipset_supported	booléen	La capacité d'agent si les ensembles d'adresses IP sont pris en charge.

Résultat de la politique concrète

Attribut	Type	Description
byte_count	int	Nombre d'octets pour les résultats de politiques concrètes.
pkt_count	int	Nombre de paquets pour les résultats des politiques concrètes.

Série chronologique du résultat de la politique concrète

Attribut	Type	Description
Horodatage	chaîne	Chaîne d'horodatage pour l'agrégation des résultats.
résultat	objet	Résultat de la politique concrète

Configuration client-serveur

La détection des relations client-serveur est au cœur de diverses fonctions de Cisco Secure Workload. C'est pourquoi nous vous recommandons d'utiliser l'agent logiciel chaque fois que cela est possible, car il peut communiquer la situation réelle. Aucun point de surveillance de la télémétrie du réseau ne peut garantir l'observation de chaque paquet pour un flux donné - en raison d'un large éventail de circonstances, par exemple : deux moitiés unidirectionnelles d'un flux TCP peuvent prendre des chemins uniques dans le réseau et seront donc toujours inévitablement affectées par un niveau d'erreur.

Cisco Secure Workload tente de détecter et de minimiser ces erreurs sans aucune interaction avec l'utilisateur en appliquant des algorithmes d'apprentissage automatique à chaque flux, en créant un modèle statistique qui fournit un jugement lorsqu'une télémétrie incohérente est signalée. Dans la majorité des cas, les utilisateurs n'ont pas à se préoccuper de cet ensemble d'API. Cependant, dans certains cas, l'algorithme de détection client-serveur n'obtient pas la bonne direction du flux. Les fonctionnalités qui dépendent de la direction du flux, par exemple la découverte automatique des politiques, peuvent présenter des comportements indésirables comme l'ouverture de ports inutiles.

Un ensemble d'API est fourni qui peut être utilisé pour fournir des conseils sur les ports de serveurs connus aux algorithmes de Cisco Secure Workload. Cet ensemble d'API est disponible pour les utilisateurs ayant le rôle de propriété de portée racine et nécessite la capacité `app_policy_management` associée à la clé API pour ces utilisateurs.

Il existe deux possibilités pour la configuration client serveur :

Configuration de l'hôte

Configuration de ports de serveur connus qui sont applicables à un sous-ensemble spécifique d'adresses IP dans une portée racine

Ajouter une configuration de port de serveur

Cette API peut être utilisée pour fournir des conseils aux algorithmes Cisco Secure Workload au sujet des ports de serveur connus pour une portée racine donnée. Vous pouvez fournir une liste de ports de serveur TCP/UDP connus pour un ensemble d'adresses IP appartenant à une portée racine afin d'aider les algorithmes Cisco Secure Workload à déterminer correctement la direction client-serveur dans les flux.

```
POST /openapi/v1/adm/{root_scope_id}/server_ports
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Identifiant unique de la portée du rôle

En outre, un fichier texte fourni comme entrée de cette API contient la configuration de port du serveur de point terminal au format suivant :

Configuration du port du serveur de point terminal

Attribut	Type	Description
ip_address	chaîne	L'adresse IP (peut être une adresse IPv4 ou IPv6). Les sous-réseaux ne sont pas autorisés.
tcp_server_ports	Liste des int	Liste des ports de serveur TCP connus correspondant à ip_address.
udp_server_ports	Liste des int	Liste des ports de serveur UDP connus correspondant à ip_address.

Configuration en bloc de ports de serveur

Attribut	Type	Description
host_config	Liste des objets de Configuration du port du serveur de point terminal .	Liste des adresses IP avec serveur connu associé ports.

Exemple de code Python

```
# contents of below file:
# {"host_config": [
#    {"ip_address": "1.1.1.1",
#     "tcp_server_ports": [100, 101, 102],
#     "udp_server_ports": [103]
#    },
#    {"ip_address": "1.1.1.2",
#     "tcp_server_ports": [200, 201, 202]
#    }
#  ]
# }

file_path = '/<path_to_file>/server_ports.txt'
root_scope_id = '<root-scope-id>'
restclient.upload(file_path,
                  '/adm/%s/server_ports' % root_scope_id,
                  timeout=200) # seconds
```

Note L'API ci-dessus écrase l'état complet de la configuration des ports de serveur connue dans le serveur principal. Si vous devez modifier quelque chose, ils doivent retélécharger la configuration complète après les modifications.

Obtenir une configuration de port de serveur

Cette API renvoie la liste des ports de serveur téléversés connus pour les points terminaux d'une portée racine.

```
GET /openapi/v1/adm/{root_scope_id}/server_ports
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Identifiant unique de la portée du rôle

Objet de réponse : une liste des objets de référence :*ServerPortConfig* .

Exemple de code Python

```
root_scope_id = '<root-scope-id>'
restclient.get('/adm/%s/server_ports' % root_scope_id)
```

Supprimer une configuration de port de serveur

Cette API supprime la configuration de port du serveur pour la portée racine spécifiée.

```
DELETE /openapi/v1/adm/{root_scope_id}/server_ports
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Identifiant unique de la portée du rôle

Objet de réponse : aucun.

Exemple de code Python

```
root_scope_id = '<root-scope-id>'
restclient.delete('/adm/%s/server_ports' % root_scope_id)
```

Configuration de port

La configuration des ports de serveur connus qui sont applicables à toutes les adresses IP qui appartiennent à une portée racine

Envoyer une configuration de port de serveur

Cette API peut être utilisée pour fournir des conseils aux algorithmes Cisco Secure Workload au sujet des ports de serveur connus pour une portée racine donnée. Les utilisateurs peuvent fournir une liste de ports de

serveur TCP/UDP connus pour une portée racine donnée afin d'aider les algorithmes de Cisco Secure Workload à déterminer la direction client-serveur correcte dans les flux. Les utilisateurs ont également la possibilité d'associer un nom de service à chaque port de serveur.

Il existe également une liste par défaut des services connus qui sont applicables à toutes les portées racine (ci-après appelés services globaux). Cette liste peut être remplacée à tout moment par l'utilisateur.

Configuration du service

Un service est défini comme une paire (port, nom).

Attribut	Type	Description
port	int	TCP/UDP server port number
name	chaîne	Nom du service associé à ce port (facultatif)
override_in_conflicts	booléen	Forcer l'hôte à être le fournisseur en cas de conflit (facultatif)

Configuration des services en masse

Attribut	Sous-attribut	Type	Description
server_ports_config	tcp_service_list	Liste des objets de *configuration de service*.	Listes des services TCP connus
	udp_service_list	Liste des objets de *configuration de service*.	Listes des services UDP connus

```
Services Push par portée racine :

POST /openapi/v1/adm/{root_scope_id}/server_ports_config
```

Exemple de code Python

```
# contents of below file:
#{"server_ports_config":
#    {
#        "tcp_service_list": [
#                {
#                        "port": 80,
#                        "name" : "http"
#
#                },
#                {
#                        "port": 53,
#                        "name" : "dns"
#                },
#                {
#                        "port": 514,
#                        "name" : "syslog",
#                        "override_in_conflicts": true
#                }
#        ],
#        "udp_service_list": [
#                {
```

```
#                         "port": 161
#                 },
#                 {
#                         "port": 53,
#                         "name": "dns"
#                 }
#         ]
#     }
#}

file_path = '/<path_to_file>/server_ports.json'

# Updating service list for a given root scope
#restclient.upload(file_path,
#                  '/openapi/v1/adm/{root_scope_id}/server_ports_config',
#                  timeout=200) # seconds
```

Note L'API ci-dessus écrase l'état complet de la configuration des ports de serveur connue dans le serveur principal. Si l'utilisateur doit modifier quelque chose, il doit télécharger à nouveau la configuration complète après les modifications.

Récupérer la configuration de port du serveur

Cette API renvoie la liste des ports de serveur connus d'une portée racine téléversée par l'utilisateur. La réponse est *Configuration de service en masse.*

```
Retrieve configured services per root scope:
    GET /openapi/v1/adm/{root_scope_id}/server_ports_config

Retrieve configured global services:
    GET /openapi/v1/adm/server_ports_config
```

Supprimer la configuration de port du serveur

Cette API supprime la configuration de port du serveur pour la portée racine spécifiée.

```
Remove configured services per root scope:
    DELETE /openapi/v1/adm/{root_scope_id}/server_ports_config
```

Agents logiciels

API des agents

Les API des agents logiciels sont associées à la gestion des agents logiciels Cisco Secure Workload. Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API. Les API *GET* ci-dessous sont également disponibles avec la capacité `flow_inventory_query` associée à la clé API.

Obtenir des agents logiciels

Ce point terminal renvoie une liste des agents logiciels. Chaque agent logiciel comporte deux champs pour décrire son type d'agent, `agent_type_str` est en texte brut tandis que `agent_type` est une énumération.

```
GET /openapi/v1/sensors
```

Paramètres :

Nom	Type	Description
limit	nombre entier	Limite le nombre de résultats renvoyés (facultatif)
offset	chaîne	Le décalage est utilisé pour les demandes paginées. Si la réponse renvoie un décalage, la requête suivante doit utiliser le même décalage pour obtenir plus de résultats sur la page suivante. (facultatif)

Obtenir un agent logiciel spécifique

Ce point terminal renvoie les attributs pour l'agent logiciel dont l'UUID fait partie de l'URI. Chaque agent logiciel comporte deux champs pour décrire son type d'agent.<agent_type_str> est en texte brut alors que<agent_type> est une énumération.

```
GET /openapi/v1/sensors/{uuid}
```

Suppression de l'agent logiciel

Ce point terminal est utilisé pour désactiver un agent logiciel en fonction de son UUID.

Utiliser l'API avec prudence; une fois qu'un agent est supprimé, il n'est plus disponible dans le tableau de bord Cisco Secure Workload et si l'agent est actif, les exportations de flux de l'agent ne sont pas autorisées dans Cisco Secure Workload.

```
DELETE /openapi/v1/sensors/{uuid}
```

Configuration de l'agent logiciel à l'aide des intents

Ce flux de travail d'API utilise quelques points terminaux REST définis ci-dessous.

Créer un filtre d'inventaire

Ce point terminal est utilisé pour préciser les critères qui correspondent aux hôtes d'agents sur lesquels l'utilisateur souhaite configurer des agents logiciels.

```
POST /openapi/v1/filters/inventories
```

Paramètres :

Nom	Type	Description
app_scope_id	chaîne	L'ID de la portée à affecter au filtre d'inventaire.
name	chaîne	Un nom pour le filtre d'inventaire
query	json	Filtre ou critères de correspondance pour l'hôte de l'agent.

Exemple de code Python

```
# app_scope_id can be retrieved by /app_scopes API
req_payload = {
   "app_scope_id": <app_scope_id>,
   "name": "sensor_config_inventory_filter",
   "query": {
      "type": "eq",
      "field": "ip",
      "value": <sensor_interface_ip>
   }
}
resp = restclient.post('/filters/inventories',
               json_body=json.dumps(req_payload)))
print resp.status_code
# returned response will contain the created filter and it's ID.
```

Création d'un profil de configuration d'agent logiciel

Ce point terminal est utilisé pour préciser l'ensemble d'options de configuration à appliquer à l'ensemble cible des agents logiciels.

```
POST /openapi/v1/inventory_config/profiles
```

Les options de configuration suivantes peuvent être spécifiées dans le profil de configuration de l'agent :

- allow_broadcast : option pour autoriser/interdire le trafic de diffusion (la valeur par défaut de cette option est True).
- allow_multicast : option pour autoriser/interdire le trafic en multidiffusion (la valeur par défaut de cette option est True).
- allow_link_local : option pour autoriser/interdire le trafic local (la valeur par défaut de cette option est True).
- auto_upgrade_opt_out : si la valeur est « vrai », les agents ne sont pas mis à niveau automatiquement lors de la mise à niveau de la grappe Cisco Secure Workload.
- cpu_quota_mode et cpu_quota_us : ces options sont utilisées pour contrôler la quantité de quota de processeur à octroyer à l'agent sur l'hôte final.
- data_plane_disabled : si la valeur est « vrai », l'agent arrête de signaler les flux à Cisco Secure Workload.
- enable_conversation_flows : option pour activer le mode conversation sur tous les agents.
- enable_forensics : option permettant d'activer la collecte des événements criminalistiques sur la charge de travail (par conséquent, l'agent utilise plus de CPU).

- enable_meltdown : active la détection d'exploit de fusion sur le charges de travail (l'agent utilise plus de CPU).
- allow_pid_lookup : si la valeur est True (vraie), l'agent tente de joindre des informations de processus aux flux. Notez que cette option de configuration utilise plus de CPU sur l'hôte final.
- enforcement_disabled : peut être utilisé pour désactiver l'application sur les hôtes exécutant des agents d'application.
- preserve_existing_rules : option pour préciser s'il faut conserver les règles iptable existantes.
- windows_enforcement_mode : option pour utiliser WAF (pare-feu avancé Windows) ou WFP (plateforme de filtrage Windows) (l'option par défaut est WAF).

Pour en savoir plus sur les options de configuration, consultez la section Configuration de l'agent logiciel .

Exemple de code Python

```
# Define profile to disable data_plane on agent
req_payload = {
   "root_app_scope_id": <root_app_scope_id>,
   "data_plane_disabled": True,
   "name": "sensor_config_profile_1",
   "enable_pid_lookup": True,
   "enforcement_disabled": False
}
resp = restclient.post('/inventory_config/profiles',
                json_body=json.dumps(req_payload))
print resp.status_code
# returned response will contain the created profile and it's ID.
parsed_resp = json.loads(resp.content)
```

Obtenir les profils de configuration d'agent logiciel

Ce point terminal renvoie une liste des profils de configuration d'agents logiciels visibles par l'utilisateur.

```
GET /openapi/v1/inventory_config/profiles
```

Paramètres : Aucun

Obtenir un profil de configuration d'agent logiciel précis

Ce point terminal renvoie une instance du profil de configuration d'agent logiciel.

```
GET /openapi/v1/inventory_config/profiles/{profile_id}
```

Renvoie l'objet de profil de configuration de l'agent logiciel associé à l'ID précisé.

Mettre à jour un profil de configuration d'agent logiciel

Ce point terminal met à jour un profil de configuration d'agent logiciel.

```
PUT /openapi/v1/inventory_config/profiles/{profile_id}
```

Les options de configuration suivantes peuvent être spécifiées dans le profil de configuration de l'agent :

- allow_broadcast : option pour autoriser/interdire le trafic de diffusion (la valeur par défaut de cette option est True).

- allow_multicast : option pour autoriser/interdire le trafic en multidiffusion (la valeur par défaut de cette option est True).
- allow_link_local : option pour autoriser/interdire le trafic local (la valeur par défaut de cette option est True).
- auto_upgrade_opt_out : si la valeur est « vrai », les agents ne sont pas mis à niveau automatiquement lors de la mise à niveau de la grappe Cisco Secure Workload.
- cpu_quota_mode et cpu_quota_us : ces options sont utilisées pour contrôler la quantité de quota de processeur à octroyer à l'agent sur l'hôte final.
- data_plane_disabled : si la valeur est « vrai », l'agent arrête de signaler les flux à Cisco Secure Workload.
- enable_conversation_flows : option pour activer le mode conversation sur tous les agents.
- enable_forensics : option permettant d'activer la collecte des événements criminalistiques sur la charge de travail (par conséquent, l'agent utilise plus de CPU).
- enable_meltdown : active la détection d'exploit de fusion sur le charges de travail (l'agent utilise plus de CPU).
- allow_pid_lookup : si la valeur est True (vraie), l'agent tente de joindre des informations de processus aux flux. Notez que cette option de configuration utilise plus de CPU sur l'hôte final.
- enforcement_disabled : peut être utilisé pour désactiver l'application sur les hôtes exécutant des agents d'application.
- preserve_existing_rules : option pour préciser s'il faut conserver les règles iptable existantes.
- windows_enforcement_mode : option pour utiliser WAF (pare-feu avancé Windows) ou WFP (plateforme de filtrage Windows) (l'option par défaut est WAF).

Pour en savoir plus sur les options de configuration, consultez la section Configuration de l'agent logiciel .

Renvoie l'objet de profil de configuration de l'agent logiciel modifié associé à l'ID précisé.

Supprimer un profil de configuration d'agent logiciel

Ce point terminal supprime le profil de configuration d'agent logiciel précisé.

```
DELETE /openapi/v1/inventory_config/profiles/{profile_id}
```

Créer un intent de configuration d'agent logiciel

Ce point terminal est utilisé pour préciser l'intention d'appliquer un ensemble d'options de configuration à un ensemble précisé d'agents logiciels. Cela créera l'intent et mettra à jour l'ordre de l'ensemble des intents en ajoutant l'intent nouvellement créé à cet ordre.

```
POST /openapi/v1/inventory_config/intents
```

Exemple de code Python

```
req_payload = {
  "inventory_config_profile_id": <>,
  "inventory_filter_id": <>
}
resp = restclient.post('/inventory_config/intents',
                json_body=json.dumps(req_payload))
```

```
print resp.status_code
# returned response will contain the created intent object and it's ID.
```

Préciser l'ordre des intents

Ce point terminal est utilisé pour préciser l'ordre des divers intents de configuration des agents logiciels. Par exemple, il peut y avoir deux intents : le premier pour activer la recherche d'ID de processus sur les ordinateurs de développement et l'autre pour désactiver la recherche d'ID de processus sur les ordinateurs Windows. Si le premier intent a une priorité plus élevée, la recherche d'ID de processus sera activée sur les ordinateurs Windows de développement. REMARQUE : Par défaut, lors de sa création, l'intent est ajouté au début de la liste de l'ordre des intents. Ce point terminal ne doit être utilisé que si l'utilisateur final doit modifier l'ordre existant des intents.

```
POST /openapi/v1/inventory_config/orders
```

Exemple de code Python

```
# Read the agent config intents ordered list
resp = restclient.get('/inventory_config/orders')
order_result_json = json.loads(resp.content)

# Modify the list by prepending the new intent in the list
order_rslt_json['intent_ids'].insert(0,<intent_id>)

# Post the new ordering back to the server
resp = restclient.post('/inventory_config/orders',
               json_body=json.dumps(order_rslt_json))
```

Supprimer l'intent de configuration de l'agent

Ce point terminal est utilisé pour supprimer un intent de configuration d'agent spécifique.

```
DELETE /openapi/v1/inventory_config/intents/{intent_id}
```

Exemple de code Python

```
intent_id = '588a51dcb5b30d0ee6da084a'
resp = restclient.delete('/inventory_config/intents/%s' % intent_id)
```

Intents de configuration d'interface

La méthode recommandée pour affecter des VRF aux agents est d'utiliser les paramètres de configuration d'un VRF distant. Dans de rares cas, lorsque les hôtes d'agents peuvent avoir plusieurs interfaces auxquelles doivent être affectées des VRF différents, les utilisateurs peuvent choisir de leur affecter des VRF à l'aide des intents de configuration d'interface. Accédez à **Manage (Gestion)** > **Agents (Agents)** et cliquez sur l'onglet **Configure (Configurer)**.

Objet intent de configuration d'inventaire

Les méthodes GET et POST renvoient un tableau d'objets JSON d'intent de configuration d'inventaire. Les attributs de l'objet sont décrits ci-dessous :

Attribut	Type	Description
vrf_id	nombre entier	valeur entière de l'ID VRF

Attribut	Type	Description
vrf_name	chaîne	Nom VRF
inventory_filter_id	chaîne	ID de filtre d'inventaire
inventory_filter	JSON	Filtre d'inventaire Consultez OpenAPI > Filtres d'inventaire pour plus de détails.

Obtenir les intents de configuration d'interface

Ce point terminal renvoie une liste des intents de configuration d'inventaire à l'utilisateur.

```
GET /openapi/v1/inventory_config/interface_intents
```

Paramètres : Aucun

Créer ou mettre à jour la liste des intents de configuration d'interface

Ce point terminal est utilisé pour créer ou modifier la liste des intents de configuration d'interface. L'API prend une liste ordonnée d'intents. Pour supprimer un intent de cette liste, les utilisateurs doivent lire la liste existante des intents, la modifier et réécrire la liste modifiée.

```
POST /openapi/v1/inventory_config/interface_intents
```

Paramètres :

Nom	Type	Description
inventory_filter_id	chaîne	ID du filtre d'inventaire correspondant à l'interface
vrf_id	nombre entier	ID VRF à attribuer à l'interface

Exemple de code Python

```
  req_payload = {
    "intents": [
      {"inventory_filter_id": <inventory_filter_id_1>, "vrf_id": <vrf_id_1>},
      {"inventory_filter_id": <inventory_filter_id_1>, "vrf_id": <vrf_id_2>}
    ]
  }
  resp = restclient.post('/inventory_config/interface_intents',
json_body=json.dumps(req_payload))
```

Configuration VRF pour les agents derrière le NAT

Les ensembles d'API suivants sont utiles pour préciser les politiques d'attribution des VRF aux agents derrière les boîtiers NAT. Ces ensembles d'API nécessitent la capacité `sensor_management` associée à la clé API et ne sont disponibles que pour les administrateurs de site.

Répertorier les règles de configuration VRF pour les agents derrière le NAT

Ce point terminal renvoie une liste des règles de configuration VRF applicables aux agents derrière le NAT.

```
GET /openapi/v1/agentnatconfig
```

Créer une nouvelle configuration VRF applicable aux agents derrière le NAT

Ce point terminal est utilisé pour préciser les critères d'étiquetage VRF pour les hôtes en fonction de leur adresse IP source et de leur port source, comme vus par l'appareil Cisco Secure Workload .

```
POST /openapi/v1/agentnatconfig
```

Paramètres :

Nom	Type	Description
src_subnet	chaîne	Sous-réseau auquel l'adresse IP source peut appartenir (notation CIDR).
src_port_range_start	nombre entier	Limite inférieure de la plage de ports source (0 à 65 535).
src_port_range_end	nombre entier	Limite supérieure de la plage du port source (0 à 65 535).
vrf_id	nombre entier	ID VRF à utiliser pour étiqueter les flux des agents dont l'adresse source et le port source se situent dans la plage précisée ci-dessus.

Exemple de code Python

```
req_payload = {
    src_subnet: 10.1.1.0/24,          # src IP range for sensors
    src_port_range_start: 0,
    src_port_range_end: 65535,
    vrf_id: 676767                    # VRF ID to assign
}

resp = rc.post('/agentnatconfig', json_body=json.dumps(req_payload))
print resp.status_code
```

Supprimer la configuration VRF existante

```
DELETE /openapi/v1/agentnatconfig/{nat_config_id}
```

Téléchargement du logiciel Cisco Secure Workload

La fonction de téléchargement de logiciel Cisco Secure Workload permet de télécharger des paquets logiciels pour les agents Cisco Secure Workload. Ces ensembles d'API nécessitent la capacité `software_download` associée à la clé API. Cette fonctionnalité est uniquement offerte aux utilisateurs administrateurs du site, aux propriétaires de la portée racine et aux utilisateurs ayant des rôles d'installation d'agent.

API pour obtenir les plateformes prises en charge

Ce point de terminaison renvoie la liste des plateformes prises en charge.

```
GET /openapi/v1/sw_assets/platforms
```

Paramètres : Aucun

Objet de réponse : renvoie la liste des plateformes prises en charge.

Exemple de code Python

L'exemple de code ci-dessous récupère toutes les plateformes prises en charge.

```
resp = restclient.get('/sw_assets/platforms')
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse

```
{"results": [{"platform": "OracleServer-6.3", "agent_type": "enforcer", "arch": "x86_64"},
 {"platform": "MSWindows8Enterprise", "agent_type": "legacy_sensor", "arch": "x86_64"}]}
```

API pour obtenir la version logicielle prise en charge

Ce point terminal renvoie la liste des versions de logiciel prises en charge pour des « type_agent », « type_de_paquet », « plateforme » et « architecture » précisés.

```
GET
/openapi/v1/sw_assets/download?platform=<platform>&agent_type=<agent_type>&pkg_type=<pkg_type>&arch=<arch>&list_version=<list_version>&installation_id=<installer_id>
```

où <agent_type> , <platform> et <arch> peuvent être l'un des résultats extraits de l' **API pour obtenir les plateformes prises en charge**, et <pkg_type> peut être « capteur_w_cfg » ou « capteur_bin_pkg ». Les deux paramètres <pkg_type> et<agent_type> sont facultatif, mais au moins l'un d'eux doit être spécifié. <list_version>doit être « True » pour activer cette API.

Paramètres : L'URL de la demande contient les paramètres suivants.

Nom	Type	Description
intégrée	chaîne	Précisez la plateforme.
agent_type	chaîne	(Facultatif) Précisez le type d'agent.
pkg_type	chaîne	(Facultatif) Précisez le type de paquet. La valeur peut être « sensor_w_cfg » ou « sensor_bin_pkg ».
arch	chaîne	Préciser l'architecture.
list_version	chaîne	Définissez la valeur « True » pour activer la recherche de version du logiciel.

Objet de réponse : renvoie une liste des versions de logiciels prises en charge.

Exemple de code Python

```
resp =
restclient.get('/sw_assets/download?platform=OracleServer-6.3&pkg_type=sensor_w_cfg&arch=x86_64&list_version=True')
if resp.status_code == 200:
   print resp.content
```

```
resp =
restclient.get('/sw_assets/download?platform=<platform>&agent_type=<agent_type>&pkg_type=<pkg_type>&arch=<arch>&sensor_version=<sensor_version>&installation_id=<installer_id>')
if resp.status_code == 200:
   print resp.content
```

Exemple de réponse

```
3.3.1.30.devel
3.3.1.31.devel
```

API pour créer l'ID du programme d'installation

Ce point terminal crée un ID d'installation pour permettre à l'API de télécharger le logiciel Cisco Secure Workload.

```
GET /openapi/v1/sw_assets/installation_id
```

Objet de réponse : renvoie un ID du programme d'installation qui peut être utilisé dans l'API pour télécharger le logiciel Cisco Secure Workload.

Exemple de code Python

```
resp = restclient.get('/sw_assets/installation_id')
if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse

```
"<installer_id>"
```

API pour télécharger le logiciel Cisco Secure Workload

Ce point terminal permet aux clients de télécharger le logiciel pour des « type-agent », « type_de_paquet », « plateforme », « architecture » et « version_capteur » précisés.

```
GET
/openapi/v1/sw_assets/download?platform=<platform>&agent_type=<agent_type>&pkg_type=<pkg_type>&arch=<arch>&sensor_version=<sensor_version>&installation_id=<installer_id>
```

où <agent_type> , <platform> et <arch> peuvent être l'un des résultats extraits de l' **API pour obtenir les plateformes prises en charge**, et <pkg_type> peut être « capteur_w_cfg » ou « capteur_bin_pkg ». Les deux paramètres <pkg_type> et<agent_type> sont facultatif, mais au moins l'un d'eux doit être spécifié. <sensor_version>peut être n'importe lequel des résultats extraits de l' **API pour obtenir la version de logiciel prise en charge**. Si « sensor_version » n'est pas spécifié, la **dernière** version du logiciel sera téléchargée.

Paramètres : L'URL de la demande contient les paramètres suivants.

Nom	Type	Description
intégrée	chaîne	Précisez la plateforme.
agent_type	chaîne	(Facultatif) Précisez le type d'agent.

Nom	Type	Description
pkg_type	chaîne	(Facultatif) Précisez le type de paquet. La valeur peut être « sensor_w_cfg » ou « sensor_bin_pkg ».
arch	chaîne	Préciser l'architecture.
sensor_version	chaîne	(Facultatif) Spécifiez la version du logiciel, la valeur par défaut est une chaîne vide.

Objet de réponse : renvoie le logiciel Cisco Secure Workload correspondant aux paramètres fournis.

Exemple de code Python

```
resp =
if resp.status_code == 200:
   print 'file downloaded successfully'
```

Mise à niveau des agents Cisco Secure Workload

La fonction de mise à niveau des agents Cisco Secure Workload permet de mettre à niveau les agents Cisco Secure Workload installés vers une version donnée. Elle met uniquement à jour les métadonnées, la mise à niveau réelle aura lieu lors du prochain enregistrement. L'API nécessite la fonctionnalité `software_download` associée à la clé API. Cette fonctionnalité est uniquement offerte aux utilisateurs administrateurs du site, aux propriétaires de la portée racine ou aux utilisateurs ayant des rôles d'installation d'agent.

API pour mettre à niveau un agent vers une version spécifique

Ce point terminal déclenche la mise à niveau de l'agent, compte tenu de sa mise à niveau « UUID » vers une « sensor_version » (version de capteur) spécifique. La dernière version sera appliquée si « sensor_version » n'est pas fourni. Cette API ne traitera pas les demandes de rétrogradation de version.

```
POST /openapi/v1/sensors/{UUID}/upgrade?sensor_version=<sensor_version>
```

où <sensor_version> peut être n'importe lequel des résultats extraits de l' API pour obtenir la version logicielle prise en charge .

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
sensor_version	chaîne	(facultatif) Précisez la version souhaitée, la dernière version sera appliquée par défaut

Renvoie l'état de cette demande de mise à niveau.

Exemple de code Python

```
resp = restclient.post('/openapi/v1/sensors/{UUID}/upgrade?sensor_version=3.4.1.1.devel')
```

```
if resp.status_code == 200:
  print 'agent upgrade was triggered successfully and in progress'
elif resp.status_code == 304:
  print 'provided version is not newer than current version'
elif resp.status_code == 400:
  print 'provided version is invalid'
elif resp.status_code == 403:
  print 'user does not have required capability'
elif resp.status_code == 404:
  print 'agent with {UUID} does not exist'
```

Règles de collecte

Cet ensemble d'API peut être utilisé pour gérer les règles de collecte. Les règles de collecte dans l'appareil Cisco Secure Workload permettent à l'utilisateur de préciser les adresses IP ou les sous-réseaux intéressants pour son déploiement. Lors de la réception de ces règles de collecte, les agents extraient uniquement les signaux de trafic pour les adresses IP qui correspondent à ces ensembles de règles de collecte. Ces API nécessitent la capacité `flow_inventory_query` associée à la clé API.

Note Ces API ne sont disponibles que pour les administrateurs du site.

Objet règle de collecte

Les attributs de l'objet règle de collecte sont décrits ci-dessous :

Attribut	Type	Description
subnet	chaîne	Sous-réseau ou adresse IP au format CIDR.
action	chaîne	Les valeurs possibles sont « INCLUDE (INCLURE) » ou « EXCLUDE (EXCLURE) ».

Mettre à jour les règles de collecte pour un VRF

Ce point terminal peut être utilisé pour mettre à jour la liste ordonnée des règles de collecte pour le VRF spécifié. Remarque : la liste des règles de collecte dans la requête POST est traitée comme une liste ordonnée.

```
POST /openapi/v1/collection_rules/{vrf_name}
```

Paramètres :

Liste ordonnée des objets règle de collecte dans le corps de la requête POST. **Les deux dernières règles doivent être les règles collectrices pour IPv4 et IPv6.** Les règles peuvent préciser les sous-réseaux 0.0.0.0/0 et::/0, respectivement, comme dans l'exemple ci-dessous.

Objet de réponse : liste ordonnée mise à jour des règles de collecte pour le VRF.

Exemple de code Python

```
req_payload = [
    {
       "subnet": "10.10.10.0/24",
       "action": "INCLUDE"
    },
    {
       "subnet": "11.11.11.0/24",
       "action": "INCLUDE"
    },
    {
       "subnet": "0.0.0.0/0",   # catch all rule for IPV4 addresses
       "action": "EXCLUDE"
    },
    {
       "subnet": "::/0",        # catch all rule for IPV6 addresses
       "action": "EXCLUDE"
    }
]
resp = restclient.post('/collection_rules/test_vrf', json_body=json.dumps(req_payload))
```

Obtenir les règles de collecte pour un VRF

Ce point terminal renvoie une liste ordonnée de règles de collecte pour un VRF spécifié.

```
GET /openapi/v1/collection_rules/{vrf_name}
```

Paramètres : Aucun

Objet de réponse : liste ordonnée des règles de collecte pour un VRF spécifié.

Exemple de code Python

```
resp = restclient.get('/collection_rules/test_vrf')
```

Incidence des règles de collecte

Il existe deux types d'éléments dans l'inventaire :

- Appris par le capteur (Profil de la charge de travail) : comprend toutes les adresses IP qui appartiennent aux charges de travail exécutant des capteurs Cisco Secure Workload
- Appris par le flux (Profil d'inventaire) : comprend toutes les adresses IP qui ont été vues dans les signaux de flux collectés par Cisco Secure Workload, mais qui ne sont associées à aucune charge de travail exécutant des agents Cisco Secure Workload.

Les règles de collecte EXCLUDE/INCLUDE contrôlent les éléments de l'inventaire qui font l'objet d'un suivi. Les éléments de l'inventaire appris par le capteur sont toujours suivis, quelles que soient les règles de collecte. Pour les éléments d'inventaire appris par le flux, s'ils sont exclus par les règles de collecte, l'élément d'inventaire n'existera pas. Par conséquent, la recherche d'inventaire ne renverra aucun résultat pour de tels inventaires.

La recherche de flux n'est pas affectée par les règles de collecte, sauf la colonne des étiquettes, qui ne sera pas remplie pour l'adresse IP exclue par les règles de collecte. Les règles de collecte n'ont aucune incidence sur la détermination du client-serveur pour un flux donné.

Les résultats de la découverte automatique des politiques peuvent être affectés, car nous ne suivons pas les étiquettes des adresses IP exclues par les règles de collecte.

Condensés de fichiers téléversés par l'utilisateur

Les utilisateurs peuvent télécharger une liste des condensés de fichiers dans Cisco Secure Workload et préciser si ces condensés sont inoffensifs ou marqués. Cisco Secure Workload signale en conséquence les processus avec les condensés binaires respectifs.

Cet ensemble d'API peut être utilisé pour charger ou supprimer une liste de condensés de fichiers dans Cisco Secure Workload. Pour appeler ces API, utilisez une clé API avec la capacité `user_data_upload`.

Note Vous pouvez avoir jusqu'à 1 million de condensés de fichiers par portée racine. 500 000 pour les condensés inoffensifs et marqués respectivement.

Les API suivantes sont à la disposition des propriétaires de la portée et des administrateurs de site et sont utilisées pour charger/télécharger/supprimer les condensés de fichiers dans une portée racine unique sur le |produit| appareil .

Téléversement du condensé de fichier par l'utilisateur

Ce point terminal est utilisé pour charger un fichier CSV avec le condensé de fichier pour une portée racine sur l'appareil Cisco Secure Workload. Les en-têtes de colonne `HashType` (type de condensé) et `FileHash` (condensé de fichier) doivent apparaître dans le fichier CSV. `HashType` doit être `SHA-1` ou `SHA-256`, FileHash ne doit pas être vide et doit être au format 40-hex SHA1 ou 64-hex SHA256.

Les en-têtes`FileName` (Nom de fichier) et `Notes` (Remarques) sont facultatifs. Le nom de fichier donné ne doit pas dépasser la longueur maximale de 150 caractères et les notes fournies ne doivent pas dépasser la longueur maximale de 1024 caractères.

```
POST /openapi/v1/assets/user_filehash/upload/{rootAppScopeNameOrID}/{benignOrflagged}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeNameOrID	chaîne	Nom ou ID de la portée racine.
benignOrflagged	chaîne	Peut être égal à `benign` (bénin) ou `flagged` (signalé).

Objet de réponse : aucun

Exemple de code Python

```
  # Sample CSV File
  # HashType,FileHash,FileName,Notes
  # SHA-1,1AF17E73721DBE0C40011B82ED4BB1A7DBE3CE29,application_1.exe,Sample Notes
  #
SHA-256,8F434346648F6B96DF89DDA901C5176B10A6D83961DD3C1AC88B59B2DC327AA4,application_2.exe,Sample
 Notes

  file_path = '/<path_to_file>/user_filehash.csv'
  root_app_scope_name = 'Tetration'
```

```
restclient.upload(file_path, '/assets/user_filehash/upload/%s/benign' % root_app_scope_name)
```

Suppression du condensé de fichier par l'utilisateur

Ce point terminal est utilisé pour charger un fichier CSV pour supprimer les condensés de fichiers de la portée racine sur l'appareil Cisco Secure Workload. Le fichier CSV doit avoir `FileHash` comme en-tête.

```
POST /openapi/v1/assets/user_filehash/delete/{rootAppScopeNameOrID}/{benignOrflagged}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeNameOrID	chaîne	Nom ou ID de la portée racine.
benignOrflagged	chaîne	Il peut s'agir de `benign (bénin)` ou `flagged` (marqué).

Objet de réponse : aucun

Exemple de code Python

```
  # Sample CSV File
  # FileHash
  # 1AF17E73721DBE0C40011B82ED4BB1A7DBE3CE29
  # 8F434346648F6B96DF89DDA901C5176B10A6D83961DD3C1AC88B59B2DC327AA4

  file_path = '/<path_to_file>/user_filehash.csv'
  root_app_scope_name = 'Tetration'
  restclient.upload(file_path, '/assets/user_filehash/delete/' + root_app_scope_name +
'/benign')
```

Téléchargement du condensé de fichier par l'utilisateur

Ce point terminal renvoie le condensé du fichier utilisateur pour la portée racine donnée sur l'appareil Cisco Secure Workload sous forme de fichier CSV. Le fichier CSV comporte les en-têtes `HashType, FileHash, FileName` et `Notes` dans l'ordre respectif.

```
GET /openapi/v1/assets/user_filehash/download/{rootAppScopeNameOrID}/{benignOrflagged}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeNameOrID	chaîne	Nom ou ID de la portée racine.
benignOrflagged	chaîne	Peut être égal à benign (bénin) ou flagged (signalé).

Objet de réponse : aucun

Exemple de code Python

```
  file_path = '/<path_to_file>/output_user_filehash.csv'
  root_app_scope_name = 'Tetration'
```

```
  restclient.download(file_path, '/assets/user_filehash/download/%s/benign' %
root_app_scope_name)
```

Étiquettes définies par l'utilisateur

Ces API sont utilisées pour ajouter ou supprimer des étiquettes définies par l'utilisateur qui libellent les flux et les éléments d'inventaire sur l'appareil Cisco Secure Workload. Pour appeler ces API, utilisez une clé API avec la capacité `user_data_upload`. Consultez la section Schéma de clé d'étiquette du guide de l'utilisateur de l'interface utilisateur pour connaître les directives régissant les clés et les valeurs utilisées pour l'étiquetage des flux et des éléments de l'inventaire.

Note Reportez-vous à la section Importation d'étiquettes personnalisées pour obtenir des instructions sur l'accès à cette fonctionnalité par l'interface utilisateur.

Note Reportez-vous aux Limites des étiquettes pour connaître les limites du nombre d'adresses IPv4/IPv6 ou de sous-réseaux qui peuvent être téléversés.

API dépendantes de la portée

Les API suivantes sont utilisées pour obtenir, définir/supprimer les étiquettes dans une portée racine sur l'appareil Cisco Secure Workload. Elles sont mises à la disposition des **propriétaires de la portée** racine et des **administrateurs de site**. En outre, les appels d'API GET sont disponibles pour les utilisateurs avec **un accès en lecture** à la portée racine.

Obtenir une étiquette d'inventaire

Ce point terminal renvoie des étiquettes pour une adresse IPv4/IPv6 ou un sous-réseau dans la portée racine sur l'appareil Cisco Secure Workload. L'adresse ou le sous-réseau utilisé pour interroger ce point terminal doivent correspondre exactement à la valeur utilisée pour le chargement des étiquettes.

```
GET /openapi/v1/inventory/tags/{rootAppScopeName}?ip={IPorSubnet}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.
IPorSubnet	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Objet de réponse :

Nom	Type	Description
attributes	JSON	Carte clé/valeur pour l'étiquetage des flux correspondants et des éléments de l'inventaire

Exemple de code Python

```
  root_app_scope_name = 'Tetration'
  restclient.get('/inventory/tags/%s' % root_app_scope_name, params={'ip': '10.1.1.1/24'})
```

Recherche d'étiquettes d'inventaire

Ce point terminal permet de rechercher des étiquettes pour une adresse IPv4/IPv6 ou un sous-réseau dans la portée racine sur l'appareil Cisco Secure Workload.

```
GET /openapi/v1/inventory/tags/{rootAppScopeName}/search?ip={IPorSubnet}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.
IPorSubnet	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Objet de réponse : cette API renvoie une liste d'objets au format suivant

Nom	Type	Description
key	chaîne	Adresse IPv4/IPv6 ou sous-réseau.
updatedAt	nombre entier	Horodatage Unix du moment où les étiquettes ont été mises à jour.
valeur	JSON	Carte clé/valeur des attributs de la clé.

Exemple de code Python

```
  root_app_scope_name = 'Tetration Scope'
  encoded_root_app_scope_name = urllib.quote(root_app_scope_name, safe='')
  restclient.get('/inventory/tags/%s/search' % encoded_root_app_scope_name, params={'ip':
'10.1.1.1/24'})
```

Définir une étiquette d'inventaire

Ce point terminal est utilisé pour définir des étiquettes pour les flux et les éléments de l'inventaire dans la portée racine sur l'appareil Cisco Secure Workload.

```
POST /openapi/v1/inventory/tags/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
ip	chaîne	Adresse IPv4/IPv6 ou sous-réseau.
attributes	JSON	Carte clé/valeur pour l'étiquetage des flux correspondants et des éléments de l'inventaire

Objet de réponse :

Nom	Type	Description
avertissements	JSON	Carte clé/valeur contenant les avertissements rencontrés lors de la définition des étiquettes.

Exemple de code Python

```
  root_app_scope_name = 'Tetration'
  req_payload = {'ip': '10.1.1.1/24', 'attributes': {'datacenter': 'SJC', 'location': 'CA'}}

  restclient.post('/inventory/tags/%s' % root_app_scope_name,
json_body=json.dumps(req_payload))
```

Supprimer les étiquettes d'inventaire

Ce point terminal supprime les étiquettes pour une adresse IPv4/IPv6 ou un sous-réseau dans une portée racine sur l'appareil Cisco Secure Workload.

```
DELETE /openapi/v1/inventory/tags/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
ip	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Exemple de code Python

```
  root_app_scope_name = 'Tetration'
  req_payload = {'ip': '10.1.1.1/24'}
  restclient.delete('/inventory/tags/%s' % root_app_scope_name,
json_body=json.dumps(req_payload))
```

Charger des étiquettes

Ce point terminal est utilisé pour charger un fichier CSV avec des étiquettes pour l'étiquetage des flux et des éléments d'inventaire dans un périmètre racine sur le l'appareil Cisco Secure Workload. Un en-tête de colonne avec le nom « `IP` » doit apparaître dans le fichier CSV. Sur les autres en-têtes de colonne, jusqu'à 32 de ces

derniers peuvent être utilisés pour annoter les flux et les éléments de l'inventaire. Pour utiliser des caractères non latins dans les étiquettes, le fichier CSV téléversé doit être au format UTF-8.

```
POST /openapi/v1/assets/cmdb/upload/{rootAppScopeName}
```

Paramètres :

L'utilisateur doit fournir un type d'opération `(X-Tetration-Oper)` en tant que paramètre de cette API. `X-Tetration-Oper` peut être l'un des éléments suivants :

- add (ajouter) : ajoute des étiquettes aux adresses ou aux sous-réseaux nouveaux et existants. Résout les conflits en sélectionnant de nouvelles étiquettes par rapport à celles existantes. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 »}*et que le fichier CSV contient *{« z » : « 1 », « bar » : « 3 »}*, *Add (Ajouter) définit les* étiquettes pour cette adresse sur *{« foo » : « 1 », « z » : « 1 », « bar » : « 3 »}*.
- overwrite (remplacer) : insère des étiquettes pour les nouvelles adresses/sous-réseaux et remplace les étiquettes pour les adresses existantes. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo » : « 1 », « bar » : « 2 »}* et que le fichier CSV contient *{« z » : « 1 », « bar » : « 3 » }*, *overwrite (remplacer)* définit les étiquettes pour cette adresse sur *{« z » : « 1 », « bar » : « 3 »}*.
- merge (fusionner) : fusionne les étiquettes avec les adresses ou les sous-réseaux existants. Résout les conflits en sélectionnant des valeurs non vides prioritairement aux valeurs vides. Par exemple, si les étiquettes d'une adresse dans la base de données sont *{« foo »: « 1 », « bar » : « 2 », « qux » : « », « corge » : « 4 »}*et que le fichier CSV contient *{« z » : « 1 », « bar » : « , « qux » : « 3 », « corge » : « 4-updated »}*, *merge (fusionner)* définit des étiquettes pour cette adresse à *{« foo » : « 1 , « z » : « 1 », « bar » : « 2 », « qux » : « 3 », « corge » : « 4-updated »}* .

Note La valeur de « bar » dans n'est pas réinitialisée à « » (vide), au lieu de cela, la valeur existante de « bar » = « 2 » est conservée.

- delete (supprimer) : supprime les étiquettes pour une adresse ou un sous-réseau.

Objet de réponse :

Nom	Type	Description
avertissements	JSON	Carte clé/valeur contenant les avertissements rencontrés lors de la définition des étiquettes.

Exemple de code Python

```
file_path = '/<path_to_file>/user_annotations.csv'
root_app_scope_name = 'Tetration'
req_payload = [tetpyclient.MultiPartOption(key='X-Tetration-Oper', val='add')]
restclient.upload(file_path, '/assets/cmdb/upload/%s' % root_app_scope_name, req_payload)
```

Charger des étiquettes au format JSON

Ce point terminal est utilisé pour charger des étiquettes pour les flux d'étiquetage et les éléments de l'inventaire sur l'appareil Cisco Secure Workload au format JSON. Les attributs dans ip_tags doivent être un sous-ensemble

d’en-têtes. Jusqu’à 32 en-têtes peuvent être utilisés pour annoter les flux et les éléments de l'inventaire. Pour utiliser des caractères non latins dans les étiquettes, la charge utile json doit être au format UTF-8.

```
POST /openapi/v1/multi_inventory/tags/{rootAppScopeName}
```

Paramètres : L’URL de la demande contient le paramètre suivant

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine

Table 74: Paramètres de la charge utile

Nom	Type	Description
headers	tableau	Tableau de chaînes de caractères spécifiant les noms des étiquettes
operation	chaîne	Soit **add** (ajouter), soit **merge** (fusionner), si ce n’est pas spécifié, l'opération est considérée comme **add**.
ip_tags	tableau	Tableau d’objets ip_tags

Table 75: ip_tags

Nom	Type	Description
ip	chaîne	Adresse IPV4/IPV6 ou sous-réseau valide
attributes	JSON	JSON de paires d'étiquettes et de chaînes de valeurs; les étiquettes doivent être un sous-ensemble d'en-têtes.

Note

1. Si les étiquettes d’enregistrement ne sont pas un sous-ensemble d’en-têtes donné, un avertissement est généré pour alerter l’utilisateur d’une différence entre les en-têtes et les étiquettes de l’enregistrement.
2. Ce point terminal ne permettra à l’utilisateur de télécharger qu’un maximum de 95 000 entrées et 36 attributs.

- Pour les demandes d’ajout, le paramètre *operation* (opération) est facultatif. S'il n’est pas spécifié, il est considéré comme **add** (ajouter).
- Pour les demandes de fusion, *operation* doit être spécifiée sous la forme **merge**.

3. Vous pouvez télécharger un maximum de 95 000 entrées et 36 attributs.

Exemple de code Python pour la demande d’ajout

```
{
```

```
    "headers" : ["key1", "key2"],
    "operation": "add"
    "ip_tags" : [
        {
            "ip": "10.10.10.11",
            "attributes": {
                "key1": "val1",
                "key2": "val2"
            }
        },
        {
            "ip": "10.10.10.12",
            "attributes": {
                "key1": "val111",
                "key2": "val2"
            }
        }
    ]
}
```

Exemple de code Python pour la demande de fusion

```
  {{
    "headers" : ["key1", "key2"],
    "operation": "merge"
    "ip_tags" : [
        {
            "ip": "10.10.10.11",
            "attributes": {
                "key1": "val1",
                "key2": "val2"
            }
        },
        {
            "ip": "10.10.10.12",
            "attributes": {
                "key1": "val1",
                "key2": "val2"
            }
        }
    ]
}
resp = restclient.post('/multi_inventory/tags/%s' % rootAppScopeName,
json_body=json.dumps(req_payload))
```

Télécharger des étiquettes utilisateur

Ce point terminal renvoie les étiquettes téléversées par l'utilisateur pour une portée racine sur l'appareil Cisco Secure Workload sous forme de fichier CSV.

```
GET /openapi/v1/assets/cmdb/download/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Réponse :

Type de contenu : *text/csv*

Fichier CSV contenant les étiquettes téléversées par l'utilisateur pour la portée.

Exemple de code Python

```
file_path = '/<path_to_file>/output.csv'
root_app_scope_name = 'Tetration'
restclient.download(file_path, '/assets/cmdb/download/%s' % root_app_scope_name)
```

Obtenir les en-têtes de colonne

Ce point terminal renvoie une liste d'en-têtes de colonne pour une portée racine sur Cisco Secure Workload.

```
GET /openapi/v1/assets/cmdb/attributenames/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Objet de réponse : un tableau des aspects disponibles pour une étiquette.

Exemple de code Python

```
root_app_scope_name = 'Tetration'
resp = restclient.get('/assets/cmdb/attributenames/%s' % root_app_scope_name)
```

Supprimer l'en-tête de colonne

Ce point terminal supprime un en-tête de colonne dans une portée racine sur l'appareil Cisco Secure Workload. La suppression d'un en-tête de colonne le supprime de la liste des aspects étiquetés et le supprime des étiquettes existantes.

```
DELETE /openapi/v1/assets/cmdb/attributenames/{rootAppScopeName}/{attributeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.
attributeName	chaîne	Attribut en cours de suppression

Objet de réponse : aucun

Exemple de code Python

```
root_app_scope_name = 'Tetration'
attribute_name = 'column1'
resp = restclient.delete('/assets/cmdb/attributenames/%s/%s' % (root_app_scope_name,
attribute_name))
```

Supprimer des étiquettes au format JSON

Ce point terminal supprime les étiquettes pour plusieurs adresses IPv4/IPv6 ou plusieurs sous-réseaux à l'aide du format JSON.

```
DELETE /openapi/v1/multi_inventory/tags/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine

Table 76: Paramètres de la charge utile

Nom	Type	Description
headers	tableau	(Facultatif) tableau de chaînes de caractères spécifiant les noms des étiquettes
ip_tags	tableau	Tableau d'objets ip_tags

Table 77: ip_tags

Nom	Type	Description
ip	chaîne	Adresse IPV4/IPV6 ou sous-réseau valide
attributes	JSON	(Facultatif) JSON de paires d'étiquettes et de chaînes de valeurs; les étiquettes doivent être un sous-ensemble d'en-têtes.

Exemple de code Python

```
  {
    "ip_tags" : [
        {
            "ip": "10.10.10.11",
          },
        {
            "ip": "10.10.10.12",
            "attributes": {
                "key1": "val1",
                "key2": "val2"
            }
        }
    ]
}
resp = restclient.delete('/multi_inventory/tags/%s' % rootAppScopeName,
json_body=json.dumps(req_payload))
```

Obtenir la liste des aspects étiquetés

Ce point terminal renvoie une liste d'aspects étiquetés pour une portée racine sur l'appareil Cisco Secure Workload. Les aspects étiquetés sont un sous-ensemble d'en-têtes de colonne dans le fichier CSV téléversé qui est utilisé pour annoter les flux et les éléments de l'inventaire dans cette portée.

```
GET /openapi/v1/assets/cmdb/annotations/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Objet de réponse : tableau d'aspects étiquetés pour la portée racine.

Exemple de code Python

```
root_app_scope_name = 'Tetration'
resp = restclient.get('/assets/cmdb/annotations/%s' % root_app_scope_name)
```

Mettre à jour la liste des aspects étiquetés

Ce point terminal met à jour la liste des aspects utilisés pour l'annotation des flux et des éléments de l'inventaire dans une portée racine sur l'appareil Cisco Secure Workload.

```
PUT /openapi/v1/assets/cmdb/annotations/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Objet de réponse : aucun

Exemple de code Python

```
# the following list is a subset of column headers in the
# uploaded CSV file
req_payload = ['location', 'region', 'detail']
root_app_scope_name = 'Tetration'
restclient.put('/assets/cmdb/annotations/%s' % root_app_scope_name,
               json_body=json.dumps(req_payload))
```

Purger les étiquettes téléversées par l'utilisateur

Ce point terminal purge les étiquettes des flux et des éléments d'inventaire dans la portée racine sur l'appareil Cisco Secure Workload. Les modifications affectent les nouvelles données; les anciennes données étiquetées demeurent inchangées.

```
POST /openapi/v1/assets/cmdb/flush/{rootAppScopeName}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
rootAppScopeName	chaîne	Nom de la portée racine.

Objet de réponse : aucun

Exemple de code Python

```
root_app_scope_name = 'Tetration'
restclient.post('/assets/cmdb/flush/%s' % root_app_scope_name)
```

API indépendantes de la portée

Les API suivantes peuvent s'étendre sur plusieurs portées sur l'appareil Cisco Secure Workload.

Note Le nombre de facettes annotées indépendantes et dépendantes de la portée ne doit pas dépasser 32 pour toute portée racine.

Charger des étiquettes

Ce point terminal est utilisé pour charger un fichier CSV avec des étiquettes pour les flux et les éléments d'inventaire sur l'appareil Cisco Secure Workload. Les en-têtes de colonne avec les noms `IP` et `VRF` doivent apparaître dans le fichier CSV, et `VRF` doit correspondre à la portée racine pour une étiquette. Sur les autres en-têtes de colonne, jusqu'à 32 de ces derniers peuvent être utilisés pour annoter les flux et les éléments de l'inventaire.

```
POST /openapi/v1/assets/cmdb/upload
```

Paramètres :

L'utilisateur doit fournir un type d'opération `(X-Tetration-Oper)` comme paramètre à cette API pour préciser l'opération à effectuer.

Objet de réponse :

Nom	Type	Description
avertissements	JSON	Matrice de clés ou de valeurs contenant les avertissements rencontrés lors de la définition des étiquettes.

Exemple de code Python

```
file_path = '/<path_to_file>/user_annotations.csv'
req_payload = [tetpyclient.MultiPartOption(key='X-Tetration-Oper', val='add')]
restclient.upload(file_path, '/assets/cmdb/upload', req_payload)
```

Télécharger des étiquettes utilisateur

Ce point terminal renvoie les étiquettes téléversées par l'utilisateur pour toutes les portées sur l'appareil Cisco Secure Workload dans un fichier CSV.

```
GET /openapi/v1/assets/cmdb/download
```

Paramètres : Aucun

Réponse :

Type de contenu : *text/csv*

Fichier CSV contenant les étiquettes téléversées par l'utilisateur pour la portée.

Exemple de code Python

```
file_path = '/<path_to_file>/output.csv'
restclient.download(file_path, '/assets/cmdb/download')
```

Étiquettes indépendantes de la portée

Ces étiquettes ne sont pas liées à une portée racine particulière et s'appliquent à toutes les portées sur l'appareil.

Obtenir une étiquette d'inventaire

Ces points terminaux renvoient des étiquettes indépendantes de la portée pour une adresse IPv4/IPv6 ou un sous-réseau sur l'appareil Cisco Secure Workload. L'adresse ou le sous-réseau utilisé pour interroger ce point terminal doit correspondre exactement à ceux utilisés pour le téléversement des étiquettes.

```
GET /openapi/v1/si_inventory/tags?ip={IPorSubnet}
```

Paramètres : L'URL de la demande contient les paramètres suivants.

Nom	Type	Description
IPorSubnet	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Objet de réponse :

Nom	Type	Description
attributes	JSON	Matrice de clés ou de valeurs pour l'étiquetage des flux et des éléments de l'inventaire correspondants

Exemple de code Python

```
restclient.get('/si_inventory/tags', params={'ip': '10.1.1.1/24'})
```

Recherche d'étiquettes d'inventaire

Ce point terminal permet de rechercher des étiquettes pour une adresse IPv4/IPv6 ou un sous-réseau sur l'appareil Cisco Secure Workload.

```
GET /openapi/v1/si_inventory/TAGs/search?ip= {IPorSubnet}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
IPorSubnet	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Objet de réponse : cette API renvoie une liste d'objets au format suivant

Nom	Type	Description
key	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Nom	Type	Description
updatedAt	nombre entier	Horodatage Unix de la mise à jour des étiquettes.
valeur	JSON	Carte de clé ou de valeur des attributs de la clé.

Exemple de code Python

```
restclient.get('/si_inventory/tags/search', params={'ip': '10.1.1.1/24'})
```

Définir une étiquette d'inventaire

Ce point terminal est utilisé pour définir des étiquettes pour les flux et les articles de l'inventaire sur l'appareil Cisco Secure Workload.

```
POST /openapi/v1/si_inventory/tags
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
ip	chaîne	Adresse IPv4/IPv6 ou sous-réseau.
attributes	JSON	Matrice de clés ou de valeurs pour l'étiquetage des flux et des éléments de l'inventaire correspondants.

Objet de réponse :

Nom	Type	Description
avertissements	JSON	Matrice de clés ou de valeurs contenant les avertissements rencontrés lors de la définition des étiquettes.

Exemple de code Python

```
req_payload = {'ip': '10.1.1.1/24', 'attributes': {'datacenter': 'SJC', 'location': 'CA'}}

restclient.post('/si_inventory/tags', json_body=json.dumps(req_payload))
```

Supprimer les étiquettes d'inventaire

Ce point terminal supprime les étiquettes pour une adresse IPv4/IPv6 ou un sous-réseau sur l'appareil Cisco Secure Workload.

```
DELETE /openapi/v1/si_inventory/tags
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
ip	chaîne	Adresse IPv4/IPv6 ou sous-réseau.

Exemple de code Python

```
req_payload = {'ip': '10.1.1.1/24'}
restclient.delete('/si_inventory/tags, json_body=json.dumps(req_payload))
```

Obtenir la liste des aspects étiquetés

Ce point terminal renvoie une liste d'attributs étiquetés indépendants de la portée sur l'appareil Cisco Secure Workload. Les aspects étiquetés sont un sous-ensemble d'en-têtes de colonnes utilisés pour annoter les flux et les éléments de l'inventaire dans tous les portées.

Note Excluez le nom de la portée de l'URL de la demande pour afficher et mettre à jour la liste des aspects annotés indépendamment de la portée.

```
GET /openapi/v1/assets/cmdb/annotations
```

Objet de réponse : un tableau de aspects étiquetés indépendants de la portée.

Exemple de code Python

```
resp = restclient.get('/assets/cmdb/annotations')
```

Mettre à jour la liste des aspects étiquetés

Ce point terminal met à jour la liste des aspects indépendants de la portée qui sont utilisés pour annoter les flux et les éléments de l'inventaire sur l'appareil Cisco Secure Workload.

```
PUT /openapi/v1/assets/cmdb/annotations
```

Objet de réponse : aucun

Exemple de code Python

```
# the following list is a subset of column headers in the
# uploaded CSV file
req_payload = ['location', 'region', 'detail']
restclient.put('/assets/cmdb/annotations',
               json_body=json.dumps(req_payload))
```

Routage et transfert virtuels

Cet ensemble d'API gère l'instance virtuelle de routage et de transmission (VRF)

Note Ces API ne sont disponibles que pour les administrateurs de site.

Objet VRF

Les attributs de l'objet VRF sont décrits ci-dessous :

Attribut	Type	Description
ID	int	Identifiant unique du VRF
name	chaîne	Nom spécifié par l'utilisateur du VRF.
tenant_id	int	ID du détenteur parent.
root_app_scope_id	chaîne	ID de la portée racine associée.
created_at	nombre entier	Horodatage Unix lors de la création du VRF.
updated_at	nombre entier	Horodatage Unix de la dernière mise à jour du VRF.

Obtenir des VRF

Ce point terminal renvoie une liste de VRF. Cette API est disponible pour les clés API avec la capacité `sensor_management ou flow_inventory_query`.

`GET /openapi/v1/vrfs`

Paramètres : Aucun

Objet de réponse : renvoie une liste des objets VRF.

Exemple de code Python

```
resp = restclient.get('/vrfs')
```

Créer un VRF

Ce point terminal est utilisé pour créer de nouveaux VRF. Une portée racine associée sera automatiquement créée avec une requête correspondant à l'ID du VRF. Cette API est disponible pour les clés API avec la capacité `sensor_management`.

`POST /openapi/v1/vrfs`

Paramètres :

Nom	Type	Description
ID	int	(Facultatif) Identifiant unique pour le VRF. Si elle n'est pas spécifiée, la grappe Cisco Secure Workload générera un ID unique pour le VRF nouvellement créé. La bonne pratique est de laisser Cisco Secure Workload générer ces ID au lieu que l'appelant spécifie explicitement des ID uniques.
tenant_id	int	(facultatif) ID du détenteur parent.
name	chaîne	Nom spécifié par l'utilisateur du VRF.
apply_monitoring_rules	booléen	(Facultatif) Indique si des règles de collecte doivent être appliquées pour le VRF. La valeur par défaut est « faux » (faux).

`tenant_id` est facultatif. S'il n'est pas fourni, le VRF sera ajouté au détenteur avec le même ID que le VRF, et il sera créé automatiquement si nécessaire. Si `tenant_id` est fourni, le locataire ne sera pas créé automatiquement et une erreur sera renvoyée s'il n'existe pas.

Objet de réponse : renvoie l'objet VRF nouvellement créé.

Exemple de code Python

```
req_payload = {
    "tenant_id": <tenant_id>,
    "name": "Test",
    "apply_monitoring_rules": True
}
resp = restclient.post('/vrfs', json_body=json.dumps(req_payload))
```

Obtenir un VRF spécifique

Ce point terminal renvoie des informations concernant l'ID de VRF spécifié. Cette API est disponible pour les clés API avec la capacité `sensor_management ou flow_inventory_query`.

```
GET /openapi/v1/vrfs/{vrf_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
vrf_id	int	Identifiant unique du VRF

Objet de réponse : renvoie un objet VRF associé à l'ID spécifié.

Exemple de code Python

```
vrf_id = 676767
resp = restclient.get('/vrfs/%d'% vrf_id)
```

Mettre à jour un VRF

Ce point terminal met à jour un VRF. Cette API est disponible pour les clés API avec la capacité `sensor_management`.

```
PUT /openapi/v1/vrfs/{vrf_id}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
vrf_id	int	Identifiant unique du VRF

Le corps de la requête JSON contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Nom spécifié par l'utilisateur du VRF.
apply_monitoring_rules	booléen	(Facultatif) Indique si les règles de collecte doivent être appliquées au VRF.

Objet de réponse : renvoie l'objet VRF modifié associé à l'ID spécifié.

Exemple de code Python

```
vrf_id = 676767
req_payload = {
    "name": "Test",
    "apply_monitoring_rules": True
}
resp = restclient.put('/vrfs/%d'% vrf_id,
                      json_body=json.dumps(req_payload))
```

Supprimer un VRF spécifique

Ce point terminal supprime un VRF. Il échoue si une portée racine est associée. Cette API est disponible pour les clés API avec la capacité `sensor_management`.

```
DELETE /openapi/v1/vrfs/{vrf_id}
```

Paramètres : le paramètre suivant fait partie de l'URL.

Nom	Type	Description
vrf_id	int	Identifiant unique du VRF

Exemple de code Python

```
vrf_id = 676767
resp = restclient.delete('/vrfs/%d'% vrf_id)
```

Orchestrateurs

Cet ensemble d'API peut être utilisé pour gérer l'apprentissage par inventaire de l'orchestrateur externe dans le déploiement de grappes Cisco Secure Workload. Elles nécessitent la capacité `external_integration` associée à la clé API.

Les types d'orchestrateurs actuellement pris en charge sont « vcenter » (vCenter 6.5 et versions ultérieures), « kubernetes », « dns », « f5 », « netscaler », « infoblox » et « Cisco FMC ». L'interface utilisateur prise en charge se trouve dans Orchestrateurs externes dans Cisco Secure Workload.

Objet orchestrateur

Les attributs de l'objet orchestrateur sont décrits ci-dessous : certains des champs ne s'appliquent qu'à des types d'orchestrateurs spécifiques; les restrictions sont mentionnées dans le tableau ci-dessous.

Attribut	Type	Description
ID	chaîne	Identifiant unique de l'orchestrateur.
name	chaîne	Nom de l'orchestrateur spécifié par l'utilisateur.
type	chaîne	Type d'orchestrateur : valeurs prises en charge (*vcenter, KUbernetes, F5, netscaler, infoblox, DNS)*
description	chaîne	Description de l'orchestrateur précisée par l'utilisateur.
username	chaîne	Nom d'utilisateur pour le point terminal de l'orchestration. (inutile pour *DNS*)
password	chaîne	Mot de passe du point terminal de l'orchestration. (inutile pour *DNS*)
certificate	chaîne	Certificat client utilisé pour l'authentification (inutile pour *DNS*)
key	chaîne	Clé correspondant au certificat client (inutile pour *DNS*)

Attribut	Type	Description
ca_certificate	chaîne	Certificat de l'autorité de certification pour valider le point terminal de l'orchestration (inutile pour *DNS*)
auth_token	chaîne	Jeton d'authentification opaque (jeton du porteur) (s'applique uniquement à *Kubernetes*)
insecure	booléen	Désactiver la vérification SSL stricte.
delta_interval	nombre entier	Délai d'interrogation de l'intervalle en secondes. Le gestionnaire d'inventaire Cisco Secure Workload effectuera une interrogation pour les modifications incrémentielles toutes les delta-interval secondes. Notez que ce paramètre ne s'applique pas à Infoblox et à Cisco Secure Firewall Management Center.
full_snapshot_interval	nombre entier	Intervalle de l'instantané complet en secondes. Le gestionnaire d'inventaire Cisco Secure Workload effectuera une interrogation d'actualisation complète à partir de l'orchestrateur
verbose_tsdb_metrics	booléen	Mesures de la TSDB par point terminal
hosts_list	Tableau	Tableau de paires { « host_name », « port_number »,} (nom de l'hôte, numéro de port) qui précisent comment Cisco Secure Workload doit se connecter à l'orchestrateur
use_secureconnector_tunnel	booléen	Connexions de tunnel vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel du connecteur sécurisé
route_domain	nombre entier	Numéro de domaine de routage à interroger sur les équilibreurs de charge F5 (s'applique uniquement à *F5*)

Attribut	Type	Description
dns_zones	Tableau	Tableau de chaînes contenant les zones DNS à interroger à partir du serveur DNS (uniquement pour *DNS*). Chaque entrée de zone DNS DOIT se terminer ainsi.
enable_enforcement	booléen	Applicable uniquement aux orchestrateurs externes avec prise en charge de l'application de la politique, tels que les pare-feu et les équilibreurs de charge. Quelques exemples : *Cisco Secure Firewall Management Center*, *F5 BIGIP* et *Citrix Netscaler*. Cet indicateur prend la valeur « faux » (l'application des politiques est désactivée) par défaut. Si la valeur est « vrai », l'orchestrateur externe déploiera les politiques sur le dispositif d'équilibreur de charge donné lors de l'application des politiques pour l'espace de travail.
ingress_controllers	objet	Tableau des objets Contrôleur d'entrée
fmc_enforcement_mode	chaîne	Applicable uniquement à *l'orchestrateur externe de Cisco Secure Firewall Management Center* et doit être soit *merge (fusion)* (par défaut) soit *override (remplacer).* La première instance indique au responsable de l'application des politiques de Cisco Secure Firewall Management Center de positionner toutes les règles de politique Cisco Secure Workload avant les règles de préfiltre existantes, tandis que la dernière instance supprimera toutes les règles de préfiltre créées par les utilisateurs.
infoblox_config	objet	Applicable uniquement à *l'orchestrateur externe Infoblox*. Sélecteurs de type d'enregistrement de Configuration Infoblox.

Contrôleur d'entrée

Attribut	Type	Description
pod_selector	objet	Sélecteur de Pod
controller_config	objet	Configuration du contrôleur

Sélecteur de Pod

Attribut	Type	Description
namespace	chaîne	L'espace de noms dans lequel le pod de contrôleur d'entrée est en cours d'exécution.
labels	Tableau	Tableau de paires {« clé », « valeur »} qui précisent les étiquettes des pods de contrôleur d'entrée.

Configuration du contrôleur

Attribut	Type	Description
ingress_class (classe_entrée)	chaîne	Nom de la classe d'entrée que le contrôleur d'entrée satisfait.
namespace	chaîne	Namespace (espace de noms) est le nom de l'espace de noms que le contrôleur d'entrée satisfait.
(http_ports) ports_http	Tableau	Tableau des ports http.
(https_ports) ports_https	Tableau	Tableau des ports https.

Configuration Infoblox

enable_network_record	booléen	La valeur par défaut est vrai. Si la valeur est Faux, les enregistrements du type *réseau* sont désactivés.
enable_host_record	booléen	La valeur par défaut est vrai. Si la valeur est Faux, les enregistrements du type *hôte* sont désactivés
enable_a_record	booléen	La valeur par défaut est vrai. Si la valeur est faux, les enregistrements de type *a* sont désactivés.

enable_aaaa_record	booléen	La valeur par défaut est vrai. Si la valeur est faux, les enregistrements de type *aaaa* sont désactivés.

** Champs d'état en lecture seule dans l'objet orchestrateur **

Attribut	Type	Description
authentication_failure	booléen	État de la connexion à l'orchestrateur Cisco Secure Workload – « *vrai* » indique une connexion réussie à l'orchestrateur. Si ce champ est *faux*, le champ *authentication_failure_error* fournira un message d'erreur détaillé expliquant la raison de l'échec d'authentification.
authentication_failure_error	chaîne	Message d'erreur détaillé pour aider à déboguer les échecs de connectivité ou d'identifiants d'authentification avec les orchestrateurs
scope_id	chaîne	ID de la portée racine du détenteur où l'inventaire sera publié et visible

Obtenir des orchestrateurs

Ce point terminal renvoie une liste des orchestrateurs connus de l'appareil Cisco Secure Workload. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/orchestrator/{scope}
```

Paramètres : Aucun

Renvoie la liste des objets orchestrateur pour la portée racine fournie. La *portée* DOIT être un ID de portée racine.

Créer des orchestrateurs

Ce point terminal est utilisé pour créer des orchestrateurs.

```
POST /openapi/v1/orchestrator/{scope}
```

Exemple de code python pour les orchestrateurs vCenter

```
req_payload = {
    "name": "VCenter Orchestrator"
    "type": "vcenter",
    "hosts_list": [ { "host_name": "8.8.8.8", "port_number": 443}],
    "username":"admin",
    "password":"admin"
```

```
}
resp = restclient.post('/orchestrator/Default', json_body=json.dumps(req_payload))
```

Exemple de code python pour les orchestrateurs DNS

```
req_payload = {
    "name": "DNS Server"
    "type": "dns",
    "hosts_list": [ { "host_name": "8.8.8.8", "port_number": 53}],
    "dns_zones": [ "lab.corp.com.", "dev.corp.com." ]
}
resp = restclient.post('/orchestrator/Default', json_body=json.dumps(req_payload))
```

Exemple de code Python pour des orchestrateurs Kubernetes

```
req_payload = {
    "name": "k8s"
    "type": "kubernetes",
    "hosts_list": [ { "host_name": "8.8.8.8", "port_number": 53}],
    "certificate": "",
    "key": "",
    "ca_certificate": "",
}
resp = restclient.post('/orchestrator/Default', json_body=json.dumps(req_payload))
```

Exemple de code python pour des orchestrateurs Kubernetes avec contrôleur d'entrée

Consultez les renseignements sur l'orchestrateur externe Kubernetes/OpenShift pour créer des renseignements détaillés d'authentification.

```
req_payload = {
    "name": "k8s",
    "type": "kubernetes",
    "hosts_list": [ { "host_name": "8.8.8.8", "port_number": 53}],
    "certificate": "",
    "key": "",
    "ca_certificate": "",
    "ingress_controllers": [
        {
            "pod_selector": {
                "namespace": "ingress-nginx",
                "labels": [{ "key": "app", "value": "nginx-ingress"}],
            }
        }
    ]
}
resp = restclient.post('/orchestrator/Default', json_body=json.dumps(req_payload))
```

Exemple de code python pour des orchestrateurs Kubernetes avec plusieurs contrôleurs d'entrée

Consultez les renseignements sur l'orchestrateur externe Kubernetes/OpenShift pour créer des renseignements détaillés d'authentification.

```
req_payload = {
    "name": "k8s",
    "type": "kubernetes",
    "hosts_list": [ { "host_name": "8.8.8.8", "port_number": 53}],
    "certificate": "",
    "key": "",
    "ca_certificate": "",
    "ingress_controllers": [
        {
```

```
                "pod_selector": {
                    "namespace": "ingress-nginx",
                    "labels": [{ "key": "app", "value": "nginx-ingress"}],
                },
                "controller_config": {
                    "ingress_class": "nginx-class",
                }
            },
            {
                "pod_selector": {
                    "namespace": "ingress-haproxy",
                    "labels": [{ "key": "app", "value": "haproxy-ingress"}],
                },
                "controller_config": {
                    "ingress_class": "haproxy-class",
                    "http_ports": [8080],
                    "https_ports": [8443],
                    "namespace": "haproxy-watching-namespace"
                }
            }
        ],
    }
    resp = restclient.post('/orchestrator/Default', json_body=json.dumps(req_payload))

    ** Type AWS and EKS are no longer supported in external orchestrators. They have been
ported to
       connectors.
```

Obtenir un orchestrateur spécifique

Ce point terminal renvoie une instance d'orchestrateur.

```
GET /openapi/v1/orchestrator/{scope}/{orchestrator_id}
```

Renvoie l'objet orchestrateur associé à l'ID spécifié.

Mettre à jour un orchestrateur

Ce point terminal met à jour un orchestrateur.

```
PUT /openapi/v1/orchestrator/{scope}/{orchestrator_id}
```

Paramètres :

Identiques aux paramètres de POST

Supprimer un orchestrateur spécifique

Ce point terminal supprime l'orchestrateur spécifié.

```
DELETE /openapi/v1/orchestrator/{scope}/{orchestrator_id}
```

Règles d'or de l'orchestrateur

Cet ensemble d'API peut être utilisé pour gérer les règles d'or pour les orchestrateurs Kubernetes externes. Des règles d'or sont nécessaires pour assurer la connectivité du plan de contrôle de Kubernetes en mode d'application de liste verte. Elles nécessitent la capacité `external_integration` associée à la clé API.

Le type d'orchestrateur actuellement pris en charge pour les règles d'or est uniquement « Kubernetes ». Les requêtes vers ce point terminal pour les orchestrateurs autres que Kubernetes échoueront.

Objet règles d'or de l'orchestrateur

Les attributs de l'objet Orchestrateur sont décrits ci-dessous :

Attribut	Type	Description
kubelet_port	nombre entier	Port d'API local au nœud de Kubelet
services	Tableau	Tableau d'objets des services Kubernetes

Obtenir les règles d'or de l'orchestrateur

Ce point terminal renvoie les règles d'or qui sont associées à un orchestrateur. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/orchestrator/{scope}/{id}/gr
```

Paramètres : Aucun

Renvoie un seul objet Règles d'or

Créer ou mettre à jour des règles d'or

Ce point terminal est utilisé pour créer ou mettre à jour les règles d'or pour un orchestrateur existant.

```
POST /openapi/v1/orchestrator/{scope}/{id}/gr
```

Paramètres :

Attribut	Type	Description
kubelet_port	nombre entier	Port d'API local au nœud de Kubelet
services	Tableau	Tableau d'objets des services Kubernetes

Exemple de code Python

```
req_payload = {
            "kubelet_port":10255,
```

```
            "services": [
                        {
    "description": "kube-dns",
    "addresses":   [ "10.0.1.1:53/TCP", "10.0.1.1:53/UDP" ],
    "consumed_by":  [ "NODES", "PODS"],
   }
             ]
  }
  resp = restclient.post('/orchestrator/{scope_id}/{orchestrator_id}/gr',
json_body=json.dumps(req_payload))
```

Domaines FMC Orchestrator

Cet ensemble d'API peut être utilisé pour gérer les domaines pour les orchestrateurs FMC externes. Les domaines FMC sont nécessaires pour activer l'application sur un domaine FMC donné. Elles nécessitent la capacité `external_integration` associée à la clé API.

Le type d'orchestrateur actuellement pris en charge pour les domaines FMC est uniquement « fmc ». Les requêtes vers ce point terminal pour les orchestrateurs autres que FMC échoueront.

Objet domaines FMC de l'orchestrateur

Les attributs de l'objet Orchestrateur sont décrits ci-dessous :

Attribut	Type	Description
fmc_domains	Tableau	Tableau d'objets de domaine FMC

Les attributs de l'objet Domaine FMC sont décrits ci-dessous :

Attribut	Type	Description
name	chaîne	Nom du domaine FMC
enforcement_enabled	booléen	Cet indicateur est défini sur False par défaut. Si la valeur est « vrai », l'orchestrateur externe déploiera les politiques sur le domaine correspondant à « name » lorsque l'application des politiques est effectuée pour l'espace de travail.

Les attributs d'URL sont décrits ci-dessous :

Attribut	Type	Description
scope	chaîne	Nom ou ID de la portée racine du détenteur où l'inventaire sera publié et visible
orchestrator_id	chaîne	ID d'orchestrateur de l'orchestrateur FMC

Obtenir les domaines FMC

Ce point terminal renvoie les domaines FMC qui sont configurés sur le FMC associé à un orchestrateur FMC. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/orchestrator/{scope}/{orchestrator_id}/fmcdomains
```

Paramètres : Aucun

Renvoie un objet JSON avec une liste d'attributs d'objet de domaine FMC.

Mettre à jour la configuration de domaine FMC pour l'orchestrateur externe FMC

Ce point terminal met à jour les attributs de domaine FMC pour un orchestrateur externe FMC existant.

```
PUT /openapi/v1/orchestrator/{scope}/{orchestrator_id}/fmcdomains
```

Paramètres :

Attribut	Type	Description
fmc_domains	Tableau	Tableau d'objets de domaine FMC

Les attributs de l'objet Domaine FMC sont décrits ci-dessous :

Attribut	Type	Description
name	chaîne	Nom du domaine FMC
enforcement_enabled	booléen	Cet indicateur est défini sur False par défaut. Si la valeur est « vrai », l'orchestrateur externe déploie des politiques sur le domaine correspondant à « name » lorsque l'application des politiques est effectuée pour l'espace de travail.

Les attributs d'URL sont décrits ci-dessous :

Attribut	Type	Description
scope	chaîne	Nom ou ID de la portée racine du détenteur où l'inventaire sera publié et visible
orchestrator_id	chaîne	ID d'orchestrateur de l'orchestrateur FMC

Exemple de code Python

```
req_payload = {
      "fmc_domains":    [
      {
```

```
            "enforcement_enabled": False,
            "name": "Global/Eng"
        },
        {
            "enforcement_enabled": True,
            "name": "Global/Prod"
        }
    ]
  }
  resp = restclient.put('/orchestrator/{scope}/{orchestrator_id}/fmcdomains',
json_body=json.dumps(req_payload))
```

Considérations relatives au contrôle d'accès en fonction des rôles (RBAC)

L'accès aux orchestrateurs sous une portée racine nécessite que la clé API utilisée pour la demande dispose des privilèges requis. Tous les appels d'API de l'orchestrateur sont déterminés et nécessitent toujours l'ID de portée racine dans l'URL. Les orchestrateurs résident toujours au niveau de la portée racine et ne peuvent pas être créés dans des sous-portées. Les orchestrateurs créés (et l'inventaire pris en charge par ces orchestrateurs) dans une portée racine de détenteur spécifique sont non vues pour les autres détenteurs.

Dans le cas des équilibreurs de charge F5 qui peuvent avoir plusieurs domaines de routage configurés (vrfs), la logique de filtrage du domaine de routage du F5 analyse toutes les entités sur F5 sur toutes les partitions, mais élimine les entités (services, bassins de paquets, pools et dorsaux) qui ne sont pas évaluées par rapport au domaine de routage spécifié dans le champ *route_domain* (domaine de routage) de l'orchestrateur F5.

Facteurs à prendre en considération concernant la haute disponibilité et le basculement

Le paramètre hosts_list permet la configuration de plusieurs adresses de serveur pour un orchestrateur. La logique de sélection du serveur Cisco Secure Workload dans le cas de plusieurs adresses de serveur varie pour chaque type d'orchestrateur.

Pour *vCenter, Kubernetes, DNS, F5, Netscaler, Infoblox*, la sélection se fait sur la base du premier point terminal intègre. Les connexions ne sont pas persistantes (sauf pour *Kubernetes*) et donc, à chaque période d'interrogation, Secure Connector Orchestrator Manager analyse les hôtes et interroge le premier point terminal intègre trouvé dans hosts_list. Pour *Kubernetes*, un canal d'événement persistant est maintenu et, en cas d'échec de la connexion, une analyse de tous les hôtes et une interrogation complète ultérieure seront effectuées à l'aide du prochain point terminal intègre.

Considérations relatives aux ressources RBAC pour Kubernetes

Le client Kubernetes tente de RECEVOIR/RÉPERTORIER/SURVEILLER les ressources suivantes.

Les informations d'authentification Kubernetes fournies doivent avoir un ensemble minimal de privilèges sur les ressources suivantes :

Ressources	Verbes
daemonsets	[obtenir la liste de surveillance]
déploiements	[obtenir la liste de surveillance]
points terminaux	[obtenir la liste de surveillance]
espaces de noms	[obtenir la liste de surveillance]
nœuds	[obtenir la liste de surveillance]
pods	[obtenir la liste de surveillance]
jeux de répliques	[obtenir la liste de surveillance]
contrôleurs de duplication	[obtenir la liste de surveillance]
services	[obtenir la liste de surveillance]
statefulsets	[obtenir la liste de surveillance]
daemonsets.apps	[obtenir la liste de surveillance]
deployments.apps	[obtenir la liste de surveillance]
endpoints.apps	[obtenir la liste de surveillance]
namespaces.apps	[obtenir la liste de surveillance]
nodes.apps	[obtenir la liste de surveillance]
pods.apps	[obtenir la liste de surveillance]
replicasets.apps	[obtenir la liste de surveillance]
replicationcontrollers.apps	[obtenir la liste de surveillance]
services.apps	[obtenir la liste de surveillance]
statefulsets.apps	[obtenir la liste de surveillance]
daemonsets.extensions	[obtenir la liste de surveillance]
deployments.extensions	[obtenir la liste de surveillance]
endpoints.extensions	[obtenir la liste de surveillance]
namespaces.extensions	[obtenir la liste de surveillance]
nœuds.extensions	[obtenir la liste de surveillance]
pods.extensions	[obtenir la liste de surveillance]
Replicasets.extensions	[obtenir la liste de surveillance]
replicationcontrollers.extensions	[obtenir la liste de surveillance]

Ressources	Verbes
services.extensions	[obtenir la liste de surveillance]
statefulsets.extensions	[obtenir la liste de surveillance]

Renseignements sur le site

Cette API peut être utilisée pour obtenir des informations sur la grappe telles que l'état de la grappe, le type de grappe, les adresses IP externes et les courriels.

Note Cette API est uniquement disponible pour les utilisateurs administrateurs du site.

Obtenir des renseignements sur le site

Ce point terminal renvoie un objet JSON avec des informations sur le site de la grappe.

```
GET /openapi/v1/site_infos
```

Paramètres : Aucun

Objet de réponse : objet JSON avec des renseignements sur le site de la grappe

Exemple de code Python

```
resp = restclient.get('/site_infos')
```

Exemple de réponse

```
{
  "cluster_state": "Enabled till 2020-12-31 23:59:59 UTC",
  "cluster_uuid": "00000000-0000-0000-0000-000000000000",
  "site_bosun_email": "customer-support@company.com",
  "site_cluster_type": "physical",
  "site_external_ips": [
      "1.1.1.1",
      "1.1.1.2",
      ...
      "1.1.1.7"
  ],
  "site_name": "cluster_name",
  "site_sensor_vip_ip": "2.1.1.1",
  "site_ui_admin_email": "site-admin@company.com",
  "site_ui_fqdn": "cluster.company.com",
  "site_ui_primary_customer_support_email": "customer-support@company.com"
}
```

État de la grappe

Cette API peut être utilisée pour obtenir l'état de tous les serveurs physiques dans Cisco Secure Workload.

Note Cette API est uniquement disponible pour les utilisateurs administrateurs du site.

Obtenir l'état d'intégrité de la grappe

Ce point terminal renvoie un objet JSON avec des informations sur l'intégrité de la grappe.

```
GET /openapi/v1/cluster_nodes
```

Paramètres : Aucun

Objet de réponse : objet JSON avec des informations sur l'intégrité de la grappe

Exemple de code Python

```
resp = restclient.get('/cluster_nodes')
```

État du service

Cette API peut être utilisée pour obtenir l'intégrité de tous les services utilisés dans la grappe Cisco Secure Workload ainsi que leurs dépendances.

Note Cette API est uniquement disponible pour les utilisateurs administrateurs du site.

Obtenir l'état d'intégrité du service

Ce point terminal renvoie un objet JSON avec des informations sur l'intégrité du service.

```
GET /openapi/v1/service_status
```

Paramètres : Aucun

Objet de réponse : objet JSON avec des renseignements sur l'intégrité du service

Exemple de code Python

```
resp = restclient.get('/service_status')
```

Connecteur sécurisé

OpenAPI affiche les points terminaux permettant de gérer les fonctions du connecteur sécurisé. Ces points terminaux nécessitent que la capacité `external_integration` soit associée à la clé API.

Note Les API du connecteur sécurisé ne peuvent pas être utilisées au niveau du site. Elles ne peuvent être utilisées qu'au niveau de la portée racine.

Obtenir l'état

Ce point terminal renvoie l'état actuel du tunnel du connecteur sécurisé pour la portée racine spécifiée.

```
GET /openapi/v1/secureconnector/name/{ROOT_SCOPE_NAME}/status
```

```
GET /openapi/v1/secureconnector/{ROOT_SCOPE_ID}/status
```

L'autorisation en lecture (READ) pour la portée racine précisée est requise.

L'état renvoyé est un objet json avec le schéma suivant :

Clé	Type	Valeur
actif	booléen	Un tunnel de connexion sécurisée (Secure Connector) est actuellement actif
peer	chaîne	<ip> :<port> de l'extrémité du tunnel client connecteur sécurisé
start_time	int	Horodatage de démarrage du tunnel (heure d'origine en secondes)
last_heartbeat	int	Horodatage de la dernière pulsation du client (heure d'origine en secondes)

Obtenir un jeton

Ce point terminal renvoie un nouveau jeton à usage unique pour une durée limitée à utiliser pour démarrer un client connecteur sécurisé pour la portée racine spécifiée.

```
GET /openapi/v1/secureconnector/name/{ROOT_SCOPE_NAME}/token
```

```
GET /openapi/v1/secureconnector/{ROOT_SCOPE_ID}/token
```

L'autorisation OWNER (PROPRIÉTAIRE) pour la portée racine précisée est requise.

Le jeton renvoyé est une chaîne qui contient un jeton signé de manière cryptographique et valide pendant une heure. Un jeton valide ne peut être utilisé qu'une seule fois pour démarrer un client connecteur sécurisé.

Alterner les certificats

Ce point terminal force la création d'un nouveau certificat pour la portée racine spécifiée. Le nouveau certificat sera utilisé par le serveur de connecteur sécurisé et sera utilisé pour signer les demandes de signature de certificat des clients pour cette portée racine.

```
POST /openapi/v1/secureconnector/name/{ROOT_SCOPE_NAME}/rotate_certs?invalidate_old=
‹→{vrai|faux}
```

```
POST /openapi/v1/secureconnector/{ROOT_SCOPE_ID}/rotate_certs?invalidate_old= ‹→{vrai|faux}
```

L'autorisation OWNER (PROPRIÉTAIRE) pour la portée racine précisée est requise.

Une fois que ce point terminal est appelé, la communication entre le client et le serveur pour cette portée racine passera immédiatement à l'utilisation du nouveau certificat.

Si *invalidate_old* est défini à False, les clients existants créent automatiquement une nouvelle paire de clés publique/privée et utilisent leurs certificats existants pour signer un nouveau certificat pour la nouvelle clé publique.

Si *invalidate_old* est défini avec True, le certificat existant est immédiatement invalidé. Les clients existants ne pourront pas se connecter au serveur et devront être redémarrés à l'aide d'un nouveau jeton. Consultez la section Déploiement du connecteur sécurisé pour de plus amples renseignements.

Analyse des vulnérabilités Kubernetes

Obtenir les registres Kubernetes utilisés pour le balayage sur les vulnérabilités des pods

Ce point terminal renvoie une liste de tous les registres Kubernetes affichés dans la grappe Cisco Secure Workload pour un VRF donné.

```
GET /openapi/kubernetes/{root_scope_name_or_id}/vulnerability_scanning/registry
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
root_scope_name_or_id	chaîne	Nom ou ID de la portée racine

Objet de réponse : renvoie un tableau d'objets de registre avec les attributs suivants :

Attribut	Type	Description
ID	chaîne	ID du registre
grappes	tableau	Tableau d'objets de grappe Kubernetes utilisant le registre
connection_status	chaîne	Définit l'état de la connexion au registre
credential_status	chaîne	État indiquant si les renseignements d'authentification sont fournis
last_scanned	Int64	Dernier analyseur à l'heure d'origine
URL	chaîne	URL du registre

Objet Grappe Kubernetes

Attribut	Type	Description
ID	chaîne	ID de la grappe Kubernetes

Attribut	Type	Description
connector_id	chaîne	ID du connecteur utilisé pour intégrer la grappe Kubernetes
connector_type	chaîne	Type de connecteur utilisé pour intégrer la grappe Kubernetes
name	chaîne	Nom de la grappe Kubernetes

Exemple de code Python

```
root_app_scope_name = 'Tetration'
restclient.get('/kubernetes/%s/vulnerability_scanning/registry' % root_app_scope_name)
```

Ajouter des informations d'authentification au registre Kubernetes

Ce point terminal vous permet d'ajouter des renseignements d'authentification sur le registre Kubernetes. Les renseignements d'authentification acceptés sont basés sur le type de registre.

Par exemple :

Type de registre : AWS; Type d'informations d'authentification acceptées : objet informations d'authentification aws_auth

Type de registre : OTHER; Type d'informations d'authentification acceptés : Objet d'authentification basic_auth

```
PUT /openapi/kubernetes/{root_scope_name_or_id}/vulnerability_scanning/registry/{registry_id}
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
root_scope_name_or_id	chaîne	Nom ou ID de la portée racine
registry_id	chaîne	ID de registre Kubernetes
registry_credential	objet	Objet identifiants

Objet identifiants

Attribut	Type	Description
basic_auth	objet	Objet authentification de base
aws_auth	objet	Objet authentification AWS
azure_auth	objet	Objet authentification Azure
gcp_auth	objet	Objet authentification GCP

basic_auth object

Attribut	Type	Description
username	chaîne	Nom d'utilisateur

Attribut	Type	Description
password	chaîne	Mot de passe

aws_auth object

Attribut	Type	Description
aws_access_key_id	chaîne	Clé d'accès aux renseignements d'authentification AWS
aws_secret_access_key	chaîne	Clé secrète d'accès aux renseignements d'authentification AWS

Objet Azur_auth :

Attribut	Type	Description
azure_tenant_id	chaîne	ID de détenteur Azure
azure_client_id	chaîne	ID du client Azure
azure_client_secret	chaîne	Code secret du client Azure

gcp_auth object:

Attribut	Type	Description
gcp_service_account	objet	Compte der service GCP

Exemple de code Python

```
root_app_scope_name = 'Tetration'
registry_id = `64cdc7a7362f57192dcc1625’
pay_load = {
        "registry_credential": {
            "basic_auth": {
                "username": "username",
                "password": "password",
            }
        }
    }
restclient.put('/kubernetes/%s/vulnerability_scanning/registry/%s' % root_app_scope_name,
registry_id, json_body=json.dumps(pay_load))
```

Obtenir les analyseurs de pods Kubernetes

Ce point terminal renvoie une liste de tous les analyseurs de pods Kubernetes affichés dans la grappe Cisco Secure Workload pour un VRF donné.

```
GET /openapi/kubernetes/{root_scope_name_or_id}/vulnerability_scanning/scanner
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
root_scope_name_or_id	chaîne	Nom ou ID de la portée racine

Objet de réponse : renvoie un tableau d'objets de registre avec les attributs suivants :

Attribut	Type	Description
ID	chaîne	ID du balayage
kubernetes_cluster	objet	Ajouter des informations d'authentification au registre Kubernetes
health_status	chaîne	Définit l'état d'intégrité de l'analyseur
health_object	chaîne	Objet d'état d'intégrité
scanner_action	chaîne	Avertit si le balayage est ACTIVÉ ou DÉSACTIVÉ
name	chaîne	Nom de l'analyseur

Objet d'intégrité

Attribut	Type	Description
last_checkin	chaîne	Dernier signalement en heure d'origine
scanner_sensor_name	chaîne	Nom du nœud Kubernetes sur lequel l'analyseur est exécuté
scanner_sensor_uuid	chaîne	ID de l'agent exécuté sur le nœud Kubernetes
état	chaîne	Avertit si l'intégrité est signalée par l'analyseur

Exemple de code Python

```
root_app_scope_name = 'Tetration'
restclient.get('/kubernetes/%s/vulnerability_scanning/scanner % root_app_scope_name)
```

Modifier la requête et l'action du filtre de l'analyseur

Ce point terminal vous permet de modifier la requête et l'action du filtre d'analyseur Kubernetes.

```
PUT /openapi/kubernetes/{root_scope_name_or_id}/vulnerability_scanning/scanner/{scanner_id}
```

Paramètres : le corps de la requête JSON contient les clés suivantes :

Nom	Type	Description
rootAppScopeName	chaîne	Nom ou ID de la portée racine
scanner_id	chaîne	ID de l'analyseur Kubernetes
scanner_action	chaîne	Pour activer ou désactiver l'analyseur. Les valeurs attendues sont ENABLED (ACTIVÉ) ou DISABLED (DÉSACTIVÉ).
filter_query	objet	Valider une requête de filtre d'inventaire pour filtrer les pods pour l'analyse des vulnérabilités.

Exemple de code Python

```
root_app_scope_name = 'Tetration'
scanner_id = '64cdc7a7362f57192dcc1625'
pay_load = {
        "scanner_action": "ENABLED"
        "filter_query": {
            "type": "contains",
            "field": "user_orchestrator_system/pod_name",
            "value": "pod"
        }
}
restclient.put('/kubernetes/%s/vulnerability_scanning/scanner/%s' % root_app_scope_name,
scanner_id, json_body=json.dumps(pay_load))
```

État d'application des politiques des orchestrateurs externes

Cet ensemble d'API est utilisé pour fournir l'état d'application des politiques pour les orchestrateurs externes de l'équilibreur de charge tels que *F5 BIG-IP* ou *Citrix Netscaler*.

Note Pour utiliser ces API, vous devez avoir accès à la portée associée au VRF.

Obtenir l'état d'application des politiques de tous les orchestrateurs externes

Ce point terminal renvoie l'état d'application de la politique pour tous les orchestrateurs externes appartenant au VRF donné. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/tnp_policy_status/{vrfID}
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
vrfID	nombre entier	ID VRF pour la portée racine.

Objet de réponse : renvoie une liste des politiques de réseau avec l'état `ENFORCED (appliqué)` ou `FAILED (échec)` ou `IGNORED (ignoré)`.

Exemple de code Python

```
vrf_id = 676767
restclient.get('/tnp_policy_status/%d' % vrf_id)
```

Obtenir l'état d'application des politiques pour un orchestrateur externe

Ce point terminal renvoie l'état d'application de la politique pour un orchestrateur externe appartenant au VRF donné. Cette API est disponible pour les clés API avec la capacité `external_integration`.

`GET /openapi/v1/tnp_policy_status/{vrfID}/{orchestratorID}`

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
vrfID	nombre entier	ID VRF pour la portée racine.
orchestratorID	chaîne	ID d'orchestrateur externe

Objet de réponse : renvoie une liste des politiques de réseau avec l'état `ENFORCED (appliqué)` ou `FAILED (échec)` ou `IGNORED (ignoré)`.

Exemple de code Python

```
vrf_id = 676767
orchestrator_id = '5ee3c991497d4f3b00f1ee07'
restclient.get('/tnp_policy_status/%d/%s' % (vrf_id, orchestrator_id))
```

Télécharger les certificats pour les surveilleurs de données et les collecteurs de données gérés

Cet ensemble d'API est utilisé pour télécharger les certificats pour les dérivateurs et les récepteurs de données gérées.

Note Pour utiliser ces API, vous devez avoir accès à la portée associée au VRF.

Obtenir la liste des surveilleurs de données gérés pour un ID VRF donné.

Ce point terminal renvoie une liste des dérivations de données gérées dans un VRF donné. Cette API est disponible pour les clés API avec la capacité `external_integration`.

`GET /openapi/v1/mdt/{vrfID}`

Paramètres : Aucun

Renvoie une liste des surveilleurs de données gérés avec des attributs tels que l'ID du surveilleur de données géré.

Télécharger des certificats de surveilleurs de données gérés pour un ID MDT donné

Ce point terminal est utilisé pour télécharger les certificats pour un ID de surveilleur de données gérées donné. L'ID MDT peut être obtenu en utilisant le point terminal **/openapi/v1/mdt/{vrfID}**, comme expliqué dans la documentation ci-dessus. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/mdt/{vrfID}/{mdtID}/certs
```

Paramètres :

Nom	Type	Description
Format	chaîne	Les formats de magasin de clés et de magasin de confiance. Valeurs : `jks`(valeur par défaut) ou `cert`

Renvoie un fichier tar.gz qui contient les fichiers suivants :

Pour le format `jks` : **truststore.jks, topic.txt, passphrase.txt, keystone.jks, kafkaBrokerIps.txt, consumer_name.txt, consumer_group_id.txt.**.

Pour le format `jks` : **KafkaConsumerCA.cert, KafkaConsumerPrivateKey.key, kafkaCA.cert, kafkaBrokerIps.txt, topic.txt**

KafkaConsumerCA.cert est le fichier de certificat public et le fichier **KafkaConsumerPrivateKey.key** contient la clé privée. **kafkaCA.cert** a le certificat d'autorité de certification et **kafkaBrokerIps.txt** a la liste des adresses IP et des ports des brokers Kafka. sujet.txt porte le nom du sujet qui doit être utilisé pour récupérer les données MDT. **truststore.jks** et **keystone.jks** sont des fichiers de magasin de clés Java.

Obtenir la liste des collecteurs de données pour un ID VRF donné

Ce point terminal renvoie une liste de récepteurs de données dans un VRF donné. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/datasinks/{vrfID}
```

Paramètres : Aucun

Renvoie une liste de récepteurs de données avec des attributs tels que l'ID de récepteur de données.

Télécharger des certificats de collecteurs de données pour un ID donné.

Ce point terminal est utilisé pour télécharger les certificats pour un ID de collecteur de données donné. L'ID de collecteur de données peut être obtenu en utilisant le point terminal **/openapi/v1/datasinks/{vrfID}**, comme expliqué dans la documentation ci-dessus. Cette API est disponible pour les clés API avec la capacité `external_integration`.

```
GET /openapi/v1/datasinks/{vrfID}/{dsID}/certs
```

Paramètres : Aucun

Renvoie un fichier tar.gz qui contient les fichiers suivants :- **userCA.cert, userPrivateKey.key, intermediateCA.cert, kafkaCA.cert, kafkaBrokerIps.txt, topic.txt**.

userCA.cert est le fichier de certificat public et le fichier **KafkaConsumerPrivateKey.key** contient la clé privée. **intermediateCA. cert** et **kafkaCA.cert** possède le certificat d'autorité de certification pour l'autorité de certification intermédiaire et racine respectivement. **kafkaBrokerIps.txt** contient la liste des adresses IP et des ports des intermédiaires Kafka. **topic.txt** porte le nom du sujet qui doit être utilisé pour récupérer les données du collecteur de données datasink.

Journaux des modifications

Cette API fournit un accès en lecture aux éléments du journal des modifications. Cette API nécessite la capacité `user_role_scope_management` associée à la clé API.

Note Cette API est uniquement disponible pour les administrateurs de site et les propriétaires de portées racine.

Objet journal des modifications

Les descriptions des attributs d'objets du journal des modifications sont les suivantes :

Attribut	Type	Description
ID	chaîne	Identifiant unique de l'élément du journal des modifications.
association_chain	tableau d'objets	Liste des noms et des ID associés à cette modification.
scope	chaîne	Portée du changement (différente d'une portée Cisco Secure Workload.
action	chaîne	Action de modification.
détails	chaîne	Plus de détails sur les actions, lorsqu'ils sont disponibles.
created_at	nombre entier	Horodatage Unix de la création de l'élément du journal des modifications.
modifier	objet	Utilisateur responsable du changement.
modifié	objet	Champs et valeurs modifiés.
initial	objet	Champs et valeurs avant modification.
version	nombre entier	Identifiant de version

Rechercher

Ce point terminal renvoie la liste des éléments du journal des modifications correspondant aux critères spécifiés.

```
GET /openapi/v1/change_logs
```

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_app_scope_id	chaîne	(Facultatif) Requis pour les propriétaires de portée racine. Filtrer les résultats par portée racine.
association_name	chaîne	(Facultatif) Requis pour les propriétaires de portée racine. Le type d'élément à retourner. Par exemple : « H4Users »
history_action	chaîne	(Facultatif) Action de modification. Par exemple : « mettre à jour »
détails	chaîne	(Facultatif) Détails de l'action. Par exemple : « suppression logicielle »
before_epoch	nombre entier	(Facultatif) Incluez les résultats créés avant cet horodatage Unix.
after_epoch	nombre entier	(Facultatif) Incluez les résultats créés depuis cet horodatage Unix.
offset	nombre entier	(facultatif) Nombre de résultats à ignorer.
limit	nombre entier	(Facultatif) Nombre limité de résultats, 1 000 par défaut.

Objet de réponse : renvoie une liste des objets du journal des modifications.

Réponse

La réponse est un objet JSON contenu dans le corps, avec les propriétés suivantes.

Nom	Type	Description
total_count	nombre entier	Nombre total d'éléments correspondants avant d'appliquer le décalage ou la limite.
Éléments	tableau d'objets	Liste des résultats.

Exemple de code Python

Récupérer les 100 dernières modifications d'objets de portée dans une portée racine donnée au cours de la dernière journée.

```
root_app_scope_id = '5ce480db497d4f1ca1fc2b2b'
one_day_ago = int(time.time() - 24*60*60)
resp = restclient.get('/change_logs', params={'root_app_scope_id': root_app_scope_id,
                                              'association_name': 'AppScope',
                                              'after_epoch': one_day_ago,
                                              'limit': 100})
```

Récupérer les deuxièmes mille modifications d'objet de portée.

```
root_app_scope_id = '5ce480db497d4f1ca1fc2b2b'
resp = restclient.get('/change_logs', params={'root_app_scope_id': root_app_scope_id,
                                              'association_name': 'AppScope',
                                              'offset': 1000})
```

Affinez davantage ces résultats pour afficher uniquement les créations de nouvelles portées.

```
root_app_scope_id = '5ce480db497d4f1ca1fc2b2b'
one_day_ago = int(time.time() - 24 * 60 * 60)
resp = restclient.get('/change_logs', params={'root_app_scope_id': root_app_scope_id,
                                              'association_name': 'AppScope',
                                              'history_action': 'create',
                                              'after_epoch': one_day_ago,
                                              'limit': 100})
```

L'administrateur d'un site peut utiliser la limite et le décalage pour récupérer de manière itérative toutes les modifications dans toutes les portées.

```
resp = restclient.get('/change_logs', params={'offset': 100, 'limit': 100})
```

Points terminaux non routables

Les API suivantes sont utilisées pour gérer les points terminaux non routables, pour marquer une adresse IP ou un sous-réseau comme non routables ou obtenir une liste des points terminaux non routables marqués par un utilisateur, ou pour désélectionner une adresse IP ou un sous-réseau comme point terminal non routable. La capacité `user_data_upload` associée à la clé API est requise.

Objet de point terminal non routable

Les descriptions des attributs de l'objet terminal non routable sont les suivantes :

Attribut	Type	Description
ID	chaîne	Identifiant unique pour le point terminal non routable.
name	chaîne	Nom spécifié par l'utilisateur du point terminal non routable.
subnet	chaîne	Sous-réseau IPv4/IPv6.
vrf_id	long	ID du VRF auquel le point terminal non routable appartient.
address_type	chaîne	IPV4/IPV6 en fonction du type d'adresse de sous-réseau
host_uuid	chaîne	Identifiant unique de l'agent

Attribut	Type	Description
description.	chaîne	Description du point terminal non routable fournie par l'utilisateur.

GET Points terminaux non routables

Ce point terminal renvoie une liste des points terminaux non routables dans le détenteur donné.

```
GET /openapi/v1/non_routable_endpoints/{rootScopeName}
```

Paramètres : Aucun

Créer un point terminal non routable

Ce point terminal est utilisé pour créer un point terminal non routable.

```
POST /openapi/v1/non_routable_endpoints/{rootScopeName}
```

Paramètres :

Attribut	Type	Description
name	chaîne	Nom spécifié par l'utilisateur du point terminal non routable.
subnet	chaîne	Le sous-réseau IPv4 ou IPv6.
address_type (facultatif)	chaîne	IPv4 ou IPv6 selon le type d'adresse de sous-réseau
host_uuid (facultatif)	chaîne	Identifiant unique de l'agent
description (facultatif)	chaîne	Description du point terminal non routable fournie par l'utilisateur.

* si les champs facultatifs ne sont pas spécifiés, des valeurs nulles sont utilisées.

Exemple de code Python

```
  req_payload = {
    "name": "nre-1",
    "subnet": "1.1.1.1/30",
    "address_type": IPV4,
    "description": "sample parameters test"
  }
  resp = restclient.post('/openapi/v1/non_routable_endpoints/Default',
json_body=json.dumps(req_payload))
```

Obtenir des points terminaux non routables spécifiques avec nom

Ce point terminal renvoie un point terminal non routable pour le nom spécifié.

```
GET /openapi/v1/non_routable_endpoints/{rootScopeName}/name/{name}
```

Paramètres : Aucun

Obtenir des points terminaux spécifiques non routables avec ID

Ce point terminal renvoie un point terminal non routable pour l'ID spécifié.

```
GET /openapi/v1/non_routable_endpoints/{rootScopeName}/id/{id}
```

Paramètres : Aucun

Mettre à jour le nom d'un point d'accès spécifique non routable

Ce point terminal est utilisé pour mettre à jour un point terminal non routable. Il utilise un ID ou un nom du point terminal non routable existant pour mettre à jour son nom.

```
PUT /openapi/v1/non_routable_endpoints/{rootScopeName}
```

Paramètres :

Attribut	Type	Description
ID	chaîne	Identifiant unique pour le point terminal non routable.
name	chaîne	Nom spécifié par l'utilisateur du point terminal non routable.
new_name	chaîne	Nouveau nom à mettre à jour

Exemple de code Python

```
  req_payload = {
    "name": "nre-1",
    "new_name": "nre-updated",
  }
  resp = restclient.put('/openapi/v1/non_routable_endpoints/Default',
json_body=json.dumps(req_payload))
```

```
  req_payload = {
    "id": "5f706964a5b5f16ed4b0aacb",
    "new_name": "nre-updated",
  }
  resp = restclient.put('/openapi/v1/non_routable_endpoints/Default',
json_body=json.dumps(req_payload))
```

Supprimer le point terminal non routable spécifique avec le nom

Ce point terminal supprime le point terminal non routable spécifique.

```
DELETE /openapi/v1/non_routable_endpoints/{rootScopeName}/name/{name}
```

Supprimer un point terminal non routable spécifique avec un ID

Ce point terminal supprime le point terminal non routable spécifique.

```
DELETE /openapi/v1/non_routable_endpoints/{rootScopeName}/id/{id}
```

Schémas de configuration et de commande pour les appareils et les connecteurs externes

API des groupes de configuration

L'API des groupes de configuration fournit des schémas de configuration pour les API des appareils et des connecteurs. Ces API nécessitent la capacité `sensor_management` ou `external_integration` qui est associée à la clé API.

API pour obtenir le schéma de configuration

Ce point terminal renvoie un schéma de configuration statique pour le type ou les groupes de configurations sélectionnés.

```
GET /openapi/v1/config_groups/schema/<type>
```

où <type> est le type de configuration de l'appareil.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
type	chaîne	Préciser le type de configuration parmi « VM1 » « VM3 » « NTP » « LOG » « LDAP » « NETFLOW » « IPFIX » « NETSCALER » « F5 » « AWS » « ENDPOINT » « SLACK_NOTIFIER » « GCP_CONNECTOR » « PAGERDUTY_NOTIFIER » « SYSLOG_NOTIFIER » « KINESIS_NOTIFIER » « EMAIL_NOTIFIER » « ISE » « MERAKI » « SLACK_NOTIFIER_OVERRIDE » « PAGERDUTY_NOTIFIER_OVERRIDE » « SYSLOG_NOTIFER_OVERRIDE » « KINESIS_NOTIFER_OVERRIDE » « AZURE_CONNECTOR » « EMAIL_NOTIFIER_OVERRIDE » « SYSLOG_SEVERITY_MAPPING » « SERVICENOW » « SYNC_INTERVAL » « ALERT » « VM3_ERSPAN » « AWS_CONNECTOR » « VM0 »

Objet de réponse : renvoie le schéma de configuration pour le type de configuration sélectionné.

Exemple de réponse

```
resp = restclient.get('/config_groups/schema/LOG')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "type": "LOG",
    "name": "Log",
    "mode": "TEST",
    "config": {
      "secured": {},
      "unsecured": {
        "log-level": "info",
        "max-log-size": 10,
        "max-log-age": 30,
        "max-log-backups": 20 }
    },
    "fill_ins": [
      {
        "field": "log-level",
        "label": "Logging Level",
        "placeholder": "info",
        "type": "user_fill_in",
        "input_type": "dropdown",
        "possible_values": [
          "trace",
          "debug",
          "info",
          "warn",
          "error"
        ]
    },
      {
        "field": "max-log-size",
        "label": "Max Log File Size (in MB)",
        "placeholder": 10,
        "type": "user_fill_in",
        "input_type": "number",
        "min": 1,
        "max": 10240
      },
      {"field": "max-log-age",
        "label": "Log Rotation (in days)",
        "placeholder": 30,
        "type": "user_fill_in",
        "input_type": "number",
        "min": 1,
        "max": 365
      },
      {
        "field": "max-log-backups",
        "label": "Log Rotation (in instances)",
        "placeholder": 20,
        "type": "user_fill_in",
        "input_type": "number",
        "min": 1,
        "max": 100
}
    ]
  }
```


API pour obtenir le schéma des commandes de dépannage

Ce point terminal renvoie un schéma de configuration de commande de dépannage statique pour le type sélectionné de commande de dépannage.

```
GET /openapi/v1/config_groups/command_schema/<type>
```

Dans la charge utile de la demande,<type> est le type de configuration de la commande de dépannage.

Paramètres :

L'URL de la demande contient les paramètres suivants

Nom	Type	Description
type	chaîne	Spécifiez le type de commande parmi "SHOW LOG" "SHOW_SERVICE_LOG" "SHOW_RUNNING_CONF" "SHOW_SERVICE_RUNNING_CONF" "SHOW_SYS_COMMANDS" "SHOW_DOCKER_COMMANDS" "SHOW_DOCKER_INSTANCE_COMMANDS" "OPER_DOCKER_INSTANCE_COMMANDS" "SHOW_SUPERVISOR_COMMANDS" "SHOW_SUPERVISOR_SERVICE_COMMANDS" "OPER_SUPERVISOR_SERVICE_COMMANDS" "NETWORK_CONNECTIVITY_COMMANDS" "LIST_FILES" "LIST_SERVICE_FILES" "PACKET_CAPTURE " "SHOW_DATA_EXPORT_LGO" "SHOW_DATAEXPORT_RUNNING_CONF" "SHOW_DATA_EXPORT_SYS_COMMANDS" "UPDATE_LISTENING_PORT" "UPDATE_TAN_LOG_CONF" "SNAPSHOT_APPLIANCE" "SNAPSHOT_CONNECTOR" "SHOW_AWS_DOWNLOADER_LOG" "CONTROLLER_PROFILING" "SERVICE_PROFILING" "RESTART_CONNECTOR_CONTAINER" "RESTART_CONNECTOR_SERVICE" "CONNECTOR_ALERT_INTERVAL_APPLIANCE" "CONNECTOR_ALERT_INTERVAL_CONNECTOR" "EXEC_SCRIPT" "SHOW_SEGMENTATION_POLICIES"

Objet de réponse : renvoie le schéma de configuration pour le type de configuration sélectionné.

Exemple de réponse

```
resp = restclient.get('/config_groups/command_schema/SHOW_LOG')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "name": "Show logs",
    "desc": "Show the contents of a log file",
   "long_desc": "Show the contents of a log file and optionally grep the file for a specified
 pattern. The output is tailed for the last 5000 lines.",
    "valid_appliances": [
      "TETRATION_DATA_INGEST",
```

```
    "TETRATION_EDGE",
    "TETRATION_EXPORT"
  ],
  "valid_connectors": [
    "netflow",
    "netscaler",
    "f5",
    "aws",
    "anyconnect",
    "slack",
    "kinesis",
    "syslog",
    "email",
    "pagerduty",
    "ise",
    "asa",
    "meraki",
    "servicenow",
    "wad"
  ],
  "arg_fillins": [
    {
      "field": "pattern",
      "label": "Grep Pattern",
      "input_type": "text",
      "optional": true
    }
  ],
  "output_type": "FILE",
  "output_ext": "LOG"
}
```

Appareils externes

API des appareils externes

Les API des appareils externes sont associées à la gestion des appareils externes SecureWorkload. Cet ensemble d'API nécessite la capacité `sensor_management` ou `external_integration` associée à la clé API.

API pour obtenir la liste des appareils

Ce point terminal renvoie la liste des appareils.

```
GET /openapi/v1/ext_appliances?root_scope_id=<root_scope_id>&type=<type>
```

où <root_scope_id> est le root_scope_id qui peut être obtenu à partir de l'API Obtenir les portées, <type> est une chaîne pour décider du type d'appareil.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Préciser la portée racine

Nom	Type	Description
type	chaîne	Préciser le type d'appareil. la valeur peut être « TETRATION_EDGE », « TETRATION_DATA_INGEST », « TETRATION_EXPORT », « TETRATION_ERSPAN » ou « TETRATION_INTERNAL »

Objet de réponse : renvoie la liste des appareils.

Exemple de réponse

```
resp =
restclient.get('/ext_appliances?root_scope_id=63bf8d2f497d4f7287dbd335&type=TETRATION_INTERNAL')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
[
    {
      "root_scope_id": "63bf8d2f497d4f7287dbd335",
      "type": "tetration_internal",
      "status": {
        "state": "active",
        "controller_state": "up",
        "message": "",
        "display_state": "active"
      },
      "auto_upgrade": true,
      "created_at": 1673498141,
      "updated_at": 1673498141,
      "registered_at": 1673498141,
      "last_checkin_at": 0,
      "last_rpm_sent_at": 0,
      "upgrade_attempts": 0,
      "delete_attempts": 0,
      "last_delete_msg_sent_at": 0,
      "taas": false,
      "deleted": false,
      "deleted_at": 0,
      "connector_limit": 5000,
      "available_slots": 5000,
      "internal": true,
      "id": "63bf8e1d6419d06bef39bc85",
      "ha_peer_appliance_id": "",
      "display_type": "Tetration Internal"
    }
  ]
```


API pour créer un appareil

Ce point terminal crée un appareil.

```
POST /openapi/v1/ext_appliances
```

Dans la charge utile de la demande, pour obtenir<config>, sélectionnez l'une des réponses « valid_config » dans API pour obtenir le schéma de l'appareil, à la page 1137, appliquez la commande « valid_config » à API pour obtenir le schéma de configuration, à la page 1124.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Précisez le nom
root_scope_id	chaîne	Préciser la portée racine
type	chaîne	Préciser le type d'appareil. la valeur peut être « TETRATION_EDGE », « TETRATION_DATA_INGEST », « TETRATION_EXPORT », « TETRATION_ERSPAN » ou « TETRATION_INTERNAL »
config (configurer)	set	Fournir le schéma de configuration rempli au format JSON
taas	booléen	Indiquez si l'appareil est conçu pour l'environnement TAAS
version	chaîne	Précisez la version

Objet de réponse : renvoie l'appareil créé.

Exemple de réponse

```
req_payload = {
    "name":"Data Ingest Appliance",
    "type":"tetration_data_ingest",
    "root_scope_id":"63c41ff2497d4f5f5be73662",
    "config":{
      "VM3":{
        "secured":{},
        "unsecured":{
          "cidr":[
            "172.26.231.141/23",
            "172.26.231.142/23",
            "172.26.231.143/23"
          ],
          "gateway":[
            "172.26.231.140",
            "172.26.231.140",
            "172.26.231.140"
          ],
          "cidr_v6":[],
          "gateway_v6":[],
          "dns":[
            "testserver"
          ],
          "search_domains":[],
          "hostname":"",
          "use_proxy_for_tetration":false,
          "https_proxy":"",
          "no_proxy":[],
          "docker_subnet":""
        }
      }
    }
  }
  resp = restclient.post('/ext_appliances', json_body=json.dumps(req_payload))
```

```
 if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse


```
{
   "root_scope_id":"63c41ff2497d4f5f5be73662",
   "type":"tetration_data_ingest",
   "status":{
     "state":"pending_dio",
     "controller_state":"down",
     "message":"Setting up appliance",
     "display_state":"preparing"
   },
   "auto_upgrade":true,
   "created_at":1674183549,
   "updated_at":1674183549,
   "registered_at":0,
   "last_checkin_at":0,
   "last_rpm_sent_at":0,
   "upgrade_attempts":0,
   "delete_attempts":0,
   "last_delete_msg_sent_at":0,
   "name":"Data Ingest Appliance",
   "taas":false,
   "deleted":false,
   "deleted_at":0,
   "connector_limit":3,
   "available_slots":0,
   "internal":false,
   "id":"63ca037dbca44e263daeb5d0",
   "ha_peer_appliance_id":"",
   "display_type":"Tetration Data Ingest"
}
```


API pour supprimer un appareil

Ce point terminal supprime l'appareil indiqué.

```
DELETE /openapi/v1/ext_appliances/<id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil

Objet de réponse : renvoie l'état de l'appareil supprimé.

Exemple de réponse

```
resp = restclient.delete('/ext_appliances/63be3b1ade36423c12bff6e1')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
{
   "status": 200,
   "code": 1000,
```

```
    "message": "deleted"
  }
```

API pour obtenir un appareil par ID

Ce point terminal obtient l'appareil à l'aide de l'ID donné.

```
GET /openapi/v1/ext_appliances/<id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil

Objet de réponse : renvoie l'appareil à l'aide de l'ID donné.

Exemple de réponse

```
resp = restclient.get('/ext_appliances/63bf8e1d6419d06bef39bc85')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "root_scope_id": "63bf8d2f497d4f7287dbd335",
    "type": "tetration_internal",
    "status": {
      "state": "active",
      "controller_state": "up",
      "message": "",
      "display_state": "active"
    },
    "auto_upgrade": true,
    "created_at": 1673498141,
    "updated_at": 1673498141,
    "registered_at": 1673498141,
    "last_checkin_at": 0,
    "last_rpm_sent_at": 0,
    "upgrade_attempts": 0,
    "delete_attempts": 0,
    "last_delete_msg_sent_at": 0,
    "taas": false,
    "deleted": false,
    "deleted_at": 0,
    "connector_limit": 5000,
    "available_slots": 5000,
    "internal": true,
    "id": "63bf8e1d6419d06bef39bc85",
    "ha_peer_appliance_id": "",
    "display_type": "Tetration Internal"
  }
```

API pour renommer un appareil

Ce point terminal renomme l'appareil à l'aide de l'ID donné.

```
PUT /openapi/v1/ext_appliances/<id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
name	chaîne	Préciser le nouveau nom de l'appareil

Objet de réponse : renvoie l'appareil avec l'ID et le nouveau nom donnés.

Exemple de réponse

```
req_payload = {
    "name": "new_name",
  }
  resp = restclient.put('/ext_appliances/63bf8e1d6419d06bef39bc85',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "root_scope_id": "63bf8d2f497d4f7287dbd335",
    "type": "tetration_internal",
    "status": {
      "state": "active",
      "controller_state": "up",
      "message": "",
      "display_state": "active"
    },
    "auto_upgrade": true,
    "created_at": 1673498141,
    "updated_at": 1673498141,
    "registered_at": 1673498141,
    "last_checkin_at": 0,
    "last_rpm_sent_at": 0,
    "upgrade_attempts": 0,
     "delete_attempts": 0,
    "last_delete_msg_sent_at": 0,
    "name": "new_name",
    "taas": false,
    "deleted": false,
    "deleted_at": 0,
    "connector_limit": 5000,
    "available_slots": 5000,
    "internal": true,
    "id": "63bf8e1d6419d06bef39bc85",
    "ha_peer_appliance_id": "",
    "display_type": "Tetration Internal"
  }
```

API pour obtenir les configurations par type de configuration

Ce point terminal obtient les configurations de l'appareil avec l'ID et le type de configuration donnés.

```
GET /openapi/v1/ext_appliances/<id>/config?config_type=<config_type>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <config_type> est la « valid_config » qui peut être obtenue à partir de API pour obtenir le schéma de l'appareil, à la page 1137.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
config_type	chaîne	Précisez le type de configuration. Reportez-vous à API pour obtenir le schéma de configuration, à la page 1124 pour toutes les valeurs possibles répertoriées dans la description

Objet de réponse : renvoie les configurations avec l'ID d'appareil et le type de configuration donnés

Exemple de réponse

```
resp =
restclient.get('/ext_appliances/63c1272039042a1c0ddd3e20/config?config_type=VM3_ERSPAN')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
[
    {
      "mode": "TEST_AND_APPLY",
      "name": "VM3_ERSPAN",
      "root_scope_id": "63bf8d2f497d4f7287dbd335",
      "vrf_id": 1,
      "appliance_id": "63c1272039042a1c0ddd3e20",
      "deleted": false,
      "type": "VM3_ERSPAN",
      "state": "COMMIT",
      "attempts": 0,
      "config": {
        "secured": {},
        "unsecured": {
          "cidr": [
            "172.26.231.141/23",
            "172.26.231.142/23",
            "172.26.231.143/23"
          ],
          "gateway": [
            "172.26.231.140",
            "172.26.231.140",
            "172.26.231.140"
          ],
          "cidr_v6": [],
          "gateway_v6": [],
          "dns": [
            "test"
          ],
          "search_domains": [],
          "hostname": "hjtest",
          "https_proxy": "",
          "no_proxy": []
        }
      },
      "push_to_dio_at": 0,
      "created_at": 1673602848,
      "updated_at": 1673602848,
```

```
    "discovery_completed_at": 0,
    "committed_at": 0,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63c1272039042a1c0ddd3e21"
  }
]
```

API pour ajouter une nouvelle configuration à un appareil externe

Ce point terminal ajoute une nouvelle configuration à l'appareil à l'aide de l'ID donné

```
POST /openapi/v1/ext_appliances/<id>/config
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127. Dans la charge utile de la demande,<type> est la « valid_config » qui peut être obtenue à partir de API pour obtenir le schéma de l'appareil, à la page 1137. Pour obtenir le schéma <config>, sélectionnez une des réponses « valid_config » dans la réponse API pour obtenir le schéma de l'appareil, à la page 1137, appliquez « valid_config » à API pour obtenir le schéma de configuration, à la page 1124.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Préciser le nom de la configuration
type	chaîne	Précisez le type de configuration. Reportez-vous à API pour obtenir le schéma de configuration, à la page 1124 pour toutes les valeurs possibles répertoriées dans la description
config (configurer)	set	Fournir le schéma de configuration rempli au format JSON

Objet de réponse : renvoie la configuration mise à jour.

Exemple de réponse

```
req_payload = {
    "name": "new_config",
    "type": "VM3_ERSPAN",
    "config": {}
  }
  resp = restclient.post('/ext_appliances/63c1272039042a1c0ddd3e20/config',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "prev_id": "63c1272039042a1c0ddd3e21",
    "mode": "TEST_AND_APPLY",
    "name": "new_config",
    "root_scope_id": "63bf8d2f497d4f7287dbd335",
```

```
    "vrf_id": 1,
    "appliance_id": "63c1272039042a1c0ddd3e20",
    "deleted": false,
    "type": "VM3_ERSPAN",
    "state": "COMMIT",
    "attempts": 0,
    "config": {
      "secured": {},
      "unsecured": null
    },
    "push_to_dio_at": 0,
    "created_at": 1673661042,
    "updated_at": 1673661042,
    "discovery_completed_at": 0,
    "committed_at": 0,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63c20a7239042a0991b871b7"
  }
```


API pour supprimer une configuration

Ce point terminal supprime une configuration d'un appareil donné.

```
DELETE /openapi/v1/ext_appliances/<id>/config/<config_id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <config_id> est l'ID qui peut être obtenu à partir de API pour obtenir les configurations par type de configuration, à la page 1132.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
config_id	chaîne	Préciser l'ID de configuration

Objet de réponse : renvoie l'état de la configuration supprimée pour l'appareil donné.

Exemple de réponse

```
resp =
restclient.delete('/ext_appliances/63c1272039042a1c0ddd3e20/config/63c1272039042a1c0ddd3e21')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
{
    "status": 200,
    "code": 1000,
    "message": "deleted"
  }
```


API pour obtenir la configuration

Ce point terminal obtient la configuration à l'aide de l'ID donné

```
GET /openapi/v1/ext_appliances/<id>/config/<config_id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <config_id> est l'ID qui peut être obtenu à partir de API pour obtenir les configurations par type de configuration, à la page 1132.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
config_id	chaîne	Préciser l'ID de configuration

Objet de réponse : renvoie la configuration à l'aide de l'ID donné.

Exemple de réponse

```
resp =
restclient.get('/ext_appliances/63c1272039042a1c0ddd3e20/config/63c1272039042a1c0ddd3e21')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
b
```

Exemple de réponse


```
{
    "mode": "TEST_AND_APPLY",
    "name": "VM3_ERSPAN",
    "root_scope_id": "63bf8d2f497d4f7287dbd335",
    "vrf_id": 1,
    "appliance_id": "63c1272039042a1c0ddd3e20",
    "deleted": false,
    "type": "VM3_ERSPAN",
    "state": "COMMIT",
    "attempts": 0,
    "config": {
      "secured": {},
      "unsecured": {
        "cidr": [
          "172.26.231.141/23",
          "172.26.231.142/23",
          "172.26.231.143/23"
        ],
        "gateway": [
          "172.26.231.140",
          "172.26.231.140",
          "172.26.231.140"
        ],
        "cidr_v6": [],
        "gateway_v6": [],
        "dns": [
          "test"
        ],
        "search_domains": [],
        "hostname": "hjtest",
        "https_proxy": "",
        "no_proxy": []
      }
    },
    "push_to_dio_at": 0,
    "created_at": 1673602848,
    "updated_at": 1673602848,
```

```
    "discovery_completed_at": 0,
    "committed_at": 0,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63c1272039042a1c0ddd3e21"
  }
```

API pour obtenir le schéma de l'appareil

Ce point terminal obtient le schéma de l'appareil d'un type donné

```
GET /openapi/v1/ext_appliances/schema/<type>
```

où <type> est une chaîne pour décider du type d'appareil.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
type	chaîne	Préciser le type d'appareil (la valeur peut être « TETRATION_EDGE », « TETRATION_DATA_INGEST », « TETRATION_EXPORT », « TETRATION_ERSPAN » ou « TETRATION_INTERNAL »

Objet de réponse : renvoie le schéma de configuration.

Exemple de réponse

```
resp = restclient.get('/ext_appliances/schema/TETRATION_ERSPAN')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
 {
    "name": "Data Ingest for ERSPAN",
    "type": "tetration_erspan",
    "desc": "Data Ingest Appliance for ERSPAN",
    "long_desc": "Data Ingest appliance for ERSPAN is a software appliance that can export
 flow data from ERSPAN appliance.",
    "valid_config": [
      "VM3_ERSPAN"
    ],
    "deploy_config": [
      "VM3_ERSPAN"
    ],
    "connectors": [
      "ERSPAN"
    ],
    "limit_connectors_per_appliance": 0,
    "limit_per_rootscope": 8,
    "limit_per_rootscope_taas": 4,
    "limit_per_cluster": 150,
    "cco_url":
"https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.26.devel"
  }
```

•

API pour répertorier les commandes de dépannage disponibles pour un appareil

Ce point terminal renvoie la liste des commandes de dépannage disponibles pour un appareil donné.

```
GET /openapi/v1/ext_appliances/<id>/commands/available
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil

Objet de réponse : renvoie la liste des commandes de dépannage disponibles pour un appareil donné.

Exemple de réponse

```
resp = restclient.get('/ext_appliances/63c6ef42bca44e2b5e729191/commands/available')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
[
    {
      "type": "UPDATE_LISTENING_PORT",
      "name": "Update the listening port on a connector"
    },
    {
      "type": "SNAPSHOT_APPLIANCE",
      "name": "Collect Snapshot from Appliance"
    },
    {
      "type": "LIST_FILES",
      "name": "List a directory"
    },
    {
      "type": "CONTROLLER_PROFILING",
      "name": "Collect controller profile"
    },
    {
      "type": "SHOW_LOG",
      "name": "Show logs"
    },
    {
      "type": "SHOW_SUPERVISOR_COMMANDS",
      "name": "Execute supervisorctl command"
    },
    {
      "type": "PACKET_CAPTURE",
      "name": "Packet capture"
    },
    {
      "type": "NETWORK_CONNECTIVITY_COMMANDS",
      "name": "Test network connectivity"
    },
    {
      "type": "SHOW_DOCKER_COMMANDS",
      "name": "Execute docker command"
    },
```

```
    {
      "type": "CONNECTOR_ALERT_INTERVAL_APPLIANCE",
      "name": "Override connector alert interval for Appliance"
    },
    {
      "type": "SHOW_RUNNING_CONF",
      "name": "Show running configuration"
    },
    {
      "type": "SHOW_SYS_COMMANDS",
      "name": "Execute system command"
    }
  ]
```

API pour lister toutes les commandes de dépannage

Ce point terminal renvoie la liste des commandes de dépannage activées pour l'appareil donné.

```
GET /openapi/v1/ext_appliances/<id>/commands
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil

Objet de réponse : renvoie la liste des commandes de dépannage activées pour l'appareil donné.

Exemple de réponse

```
resp = restclient.get('/ext_appliances/63be3b1ade36423c12bff6e1/commands')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
[
    {
      "appliance_id": "63be3b1ade36423c12bff6e1",
      "state": "pending",
      "level": "APPLIANCE",
      "command": "SHOW_LOG",
      "arg_string": "",
      "args": {},
      "tailed": false,
      "rc": 0,
      "push_to_dio_at": 0,
      "attempts": 0,
      "deleted": false,
      "deleted_at": 0,
      "created_at": 1673595392,
      "total_chunk": 0,
      "id": "63c10a0039042a6aee1b008c"
    }
  ]
```

API pour créer une commande de dépannage

Ce point terminal crée une commande de dépannage disponible pour un appareil donné.

```
POST /openapi/v1/ext_appliances/<id>/commands
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127. Dans la charge utile de la demande,<command> est un type de commande de dépannage qui peut être obtenu à partir du champ « valid_appliances » de la réponse API pour obtenir le schéma des commandes de dépannage, à la page 1125. <arguments>est un objet JSON contenant le schéma de commande, qui peut être obtenu à partir de API pour obtenir le schéma des commandes de dépannage, à la page 1125.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
commande	chaîne	Préciser le type de commande
arguments	set	Fournir le schéma de commande rempli au format JSON

Objet de réponse : renvoie la commande de dépannage créée pour l'appareil donné.

Exemple de réponse

```
req_payload = {
    "command": "SHOW_LOG",
    "arguments": {}
  }
  resp = restclient.post('/ext_appliances/63be3b1ade36423c12bff6e1/commands',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "appliance_id": "63be3b1ade36423c12bff6e1",
    "state": "pending",
    "level": "APPLIANCE",
    "command": "SHOW_LOG",
    "args": {},
    "tailed": false,
    "rc": 0,
    "push_to_dio_at": 0,
    "attempts": 0,
    "deleted": false,
    "deleted_at": 0,
    "created_at": 1673595392,
    "total_chunk": 0,
    "id": "63c10a0039042a6aee1b008c"
  }
```

-

API pour supprimer une commande de dépannage

Ce point terminal supprime une commande de dépannage activée pour l'appareil donné.

```
DELETE /openapi/v1/ext_appliances/<id>/commands/<command_id>
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <command_id> est l'ID qui peut être obtenu à partir de API pour lister toutes les commandes de dépannage, à la page 1139.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : renvoie l'état de la commande de dépannage supprimée pour l'appareil donné.

Exemple de réponse

```
resp =
restclient.delete('/ext_appliances/63be3b1ade36423c12bff6e1/commands/63c10a0039042a6aee1b008c')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
 {
    "status": 200,
    "code": 1000,
    "message": "deleted"
  }
```

API pour renvoyer une commande de dépannage

Ce point terminal renvoie la commande de dépannage sélectionnée pour un appareil donné.

```
GET /openapi/v1/ext_appliances/<id>/commands/<command_id>
```

où <id> est l'appareil_id obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <command_id> est l'ID obtenu de API pour lister toutes les commandes de dépannage, à la page 1139.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : renvoie la commande de dépannage sélectionnée pour un appareil donné.

Exemple de réponse

```
resp =
restclient.get('/ext_appliances/63be3b1ade36423c12bff6e1/commands/63c10fd139042a1c0ddd3e1f')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "appliance_id": "63be3b1ade36423c12bff6e1",
    "state": "pending",
    "level": "APPLIANCE",
    "command": "SHOW_LOG",
    "arg_string": "",
```

```
    "args": {},
    "tailed": false,
    "rc": 0,
    "push_to_dio_at": 0,
    "attempts": 0,
    "deleted": false,
    "deleted_at": 0,
    "created_at": 1673596881,
    "total_chunk": 0,
    "id": "63c10fd139042a1c0ddd3e1f"
}
```


API pour télécharger la sortie de la commande de l'appareil sous forme de fichier

Ce point terminal télécharge la sortie de la commande en tant que fichier.

```
GET /openapi/v1/appliances/<id>/commands/{command_id}/download
```

où <id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <command_id> est l'ID qui peut être obtenu à partir de API pour lister toutes les commandes de dépannage, à la page 1139. Toutes les commandes n'ont pas une sortie téléchargeable, vérifiez le schéma de commande fourni par API pour obtenir le schéma des commandes de dépannage, à la page 1125, où « output_type » : « FILE » indique que du contenu est téléchargeable et « output_ext » indique le type de fichier.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : téléchargez le résultat de la commande sous forme de fichier.

Exemple de réponse

```
resp = restclient.download('downloadFile',
'/appliances/63c6ef42bca44e2b5e729191/commands/63cace941a49bd4c0e0cf45a/download')
```

Connecteurs

API de connecteurs

Les API des connecteurs sont associées à la gestion des connecteurs de Cisco Secure Workload. Cet ensemble d'API nécessite la capacité `sensor_management` ou `external_integration` associée à la clé API.

API pour obtenir tous les types de connecteurs

Ce point terminal obtient tous les types de connecteurs d'une portée racine donnée.

```
GET /openapi/v1/connectors/cards?root_scope_id=<root_scope_id>
```

où <root_scope_id> est le root_scope_id qui peut être obtenu à partir de l'API Obtenir les portées, à la page 997.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Préciser la portée racine

Objet de réponse : renvoie tous les types de connecteurs avec un ID de portée racine donné.

Exemple de réponse

```
resp = restclient.get('/connectors/cards?root_scope_id=63bf8d2f497d4f7287dbd335')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
[{
    "type": "NETFLOW",
    "name": "NetFlow",
    "desc": "Collect telemetry from network devices",
    "long_desc": "Collect NetFlow V9 and/or IPFIX telemetry from network devices such as
routers and switches.",
    "group": "Flow Ingest",
    "index": 0,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 3,
    "limit_per_rootscope": 10,
    "limit_per_cluster": 100,
    "config": [
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility"
    ],
    "connector_count": 0,
    "group_order": 0
  },
  {
    "type": "NETSCALER",
    "name": "NetScaler",
    "desc": "Collect telemetry from Citrix ADC",
   "long_desc": "Collect telemetry from Citrix ADC, stitch client and server side flows.",

    "group": "Flow Ingest",
    "index": 2,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 3,
    "limit_per_rootscope": 10,
    "limit_per_cluster": 100,
    "config": [
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "Flow Stitching",
      "ADM"
    ],
    "connector_count": 0,
    "group_order": 0
  },
```

```
  {
    "type": "F5",
    "name": "F5",
    "desc": "Collect telemetry from F5 BIG-IP",
    "long_desc": "Collect telemetry from F5 BIG-IP, stitch client and server side flows,
enrich client inventory with user attributes.",
    "group": "Flow Ingest",
    "index": 1,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 3,
    "limit_per_rootscope": 10,
    "limit_per_cluster": 100,
    "config": [
      "LDAP",
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "User Insights",
      "Flow Stitching",
      "ADM"
    ],
    "connector_count": 0,
    "group_order": 0
  },
  {
    "type": "ANYCONNECT",
    "name": "AnyConnect",
    "desc": "Collect telemetry from AnyConnect NVM",
    "long_desc": "Collect telemetry data from Cisco AnyConnect Network Visibility Module
(NVM) and enrich endpoint inventories with user attributes",
    "group": "Endpoints",
    "index": 0,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 50,
    "limit_per_cluster": 500,
    "config": [
      "ENDPOINT",
      "LDAP",
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "Process Annotation",
      "User Insights",
      "Endpoint Insights",
      "Inventory Enrichment"
    ],
    "connector_count": 0,
    "group_order": 1
  },
  {
    "type": "ASA",
```

```
    "name": "Cisco Secure Firewall",
    "desc": "Collect telemetry from Cisco Secure Firewall",
    "long_desc": "Collect telemetry from Cisco Secure Firewall, stitch client and server
side flows. Recommended usage with ISE connector for flow visibility.",
    "group": "Flow Ingest",
    "index": 3,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 10,
    "limit_per_cluster": 100,
    "config": [
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "Flow Stitching",
      "ADM"
    ],
    "connector_count": 0,
    "group_order": 0
  },
  {
    "type": "SLACK",
    "name": "Slack",
    "desc": "Send alerts to Slack",
    "long_desc": "Send Tetration Alerts to Slack.",
    "group": "Alerts",
    "index": 2,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "SLACK_NOTIFIER",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Alert Destination"
    ],
    "connector_count": 0,
    "group_order": 3
  },
  {
    "type": "KINESIS",
    "name": "Kinesis",
    "desc": "Send alerts to Kinesis",
    "long_desc": "Send Tetration Alerts to Kinesis.",
    "group": "Alerts",
    "index": 4,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
```

```
      "KINESIS_NOTIFIER",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Alert Destination"
    ],
    "connector_count": 0,
    "group_order": 3
  },
  {
    "type": "SYSLOG",
    "name": "Syslog",
    "desc": "Send alerts to Syslog server",
    "long_desc": "Send Tetration Alerts to Syslog server.",
    "group": "Alerts",
    "index": 0,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "SYSLOG_NOTIFIER",
      "SYSLOG_SEVERITY_MAPPING",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Alert Destination"
    ],
    "connector_count": 0,
    "group_order": 3
  },
  {
    "type": "EMAIL",
    "name": "Email",
    "desc": "Send alerts to Email",
    "long_desc": "Send Tetration Alerts to Email.",
    "group": "Alerts",
    "index": 1,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "EMAIL_NOTIFIER",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Alert Destination"
    ],
    "connector_count": 0,
    "group_order": 3
  },
  {
```

```
    "type": "PAGERDUTY",
    "name": "Pager Duty",
    "desc": "Send alerts to Pager Duty",
    "long_desc": "Send Tetration Alerts to Pager Duty",
    "group": "Alerts",
    "index": 3,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "PAGERDUTY_NOTIFIER",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Alert Destination"
    ],
    "connector_count": 0,
    "group_order": 3
  },
  {
    "type": "ISE",
    "name": "ISE",
    "desc": "Collect endpoints and inventories from Cisco ISE",
    "long_desc": "Collect information about endpoints and inventories managed by Cisco ISE
 appliances and enrich endpoint inventories with user attributes and secure group tags
(SGT). Recommended usage with Cisco Secure Firewall connector for flow visibility.",
    "group": "Endpoints",
    "index": 1,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "LDAP",
      "LOG",
      "ALERT"
    ],
    "instance_spec": "ISE",
    "max_instances": 20,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "User Insights",
      "Inventory Enrichment",
      "Endpoint Insights",
      "Software Compliance Posture",
      "MDM Insights"
    ],
    "connector_count": 0,
    "group_order": 1
  },
  {
    "type": "MERAKI",
    "name": "Meraki",
    "desc": "Collect telemetry from Meraki firewalls",
    "long_desc": "Collect telemetry data from Meraki firewalls.",
    "group": "Flow Ingest",
    "index": 5,
```

```
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 10,
    "limit_per_cluster": 100,
    "config": [
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility"
    ],
    "connector_count": 0,
    "group_order": 0
  },
  {
    "type": "SERVICENOW",
    "name": "ServiceNow",
    "desc": "Collect ServiceNow CMDB records for inventories",
   "long_desc": "Collect CMDB information and service records from ServiceNow instance and
enriches endpoint inventories with cmdb attributes.",
    "group": "Inventory Enrichment",
    "index": 1,
    "appliance_type": "tetration_edge",
    "state": "disabled",
    "limit_per_appliance": 1,
    "limit_per_rootscope": 1,
    "limit_per_cluster": 150,
    "config": [
      "SERVICENOW",
      "SYNC_INTERVAL",
      "LOG",
      "ALERT"
    ],
    "instance_spec": "SERVICENOW",
    "max_instances": 10,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "User Insights",
      "Inventory Enrichment",
      "Endpoint Insights",
      "Software Compliance Posture"
    ],
    "connector_count": 0,
    "group_order": 2
  },
  {
    "type": "ERSPAN",
    "name": "ERSPAN",
    "desc": "Collect ERSPAN traffic",
    "long_desc": "",
    "group": "Flow Ingest",
    "index": 7,
    "appliance_type": "tetration_erspan",
    "state": "enabled",
    "limit_per_appliance": 3,
    "limit_per_rootscope": 24,
    "limit_per_cluster": 450,
    "config": [],
    "max_instances": 0,
```

```
    "noteworthy": false,
    "hidden": false,
    "capabilities": [],
    "connector_count": 3,
    "group_order": 0
  },
  {
    "type": "AWS_CONNECTOR",
    "name": "AWS",
    "desc": "AWS Connector",
    "long_desc": "",
    "group": "Cloud",
    "index": 0,
    "appliance_type": "tetration_internal",
    "state": "disabled",
    "limit_per_appliance": 5000,
    "limit_per_rootscope": 5000,
    "limit_per_cluster": 100000,
    "config": [
      "AWS_CONNECTOR"
    ],
    "max_instances": 0,
    "noteworthy": true,
    "pre_release_tag": "BETA",
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "Segmentation",
      "Managed K8s",
      "Inventory Enrichment"
    ],
    "connector_count": 0,
    "group_order": 5
  },
  {
    "type": "AZURE_CONNECTOR",
    "name": "Azure",
    "desc": "Azure Connector",
    "long_desc": "",
    "group": "Cloud",
    "index": 1,
    "appliance_type": "tetration_internal",
    "state": "disabled",
    "limit_per_appliance": 5000,
    "limit_per_rootscope": 5000,
    "limit_per_cluster": 100000,
    "config": [
      "AZURE_CONNECTOR"
    ],
    "max_instances": 0,
    "noteworthy": true,
    "pre_release_tag": "BETA",
    "hidden": false,
    "capabilities": [
      "Flow Visibility",
      "Segmentation",
      "Managed K8s",
      "Inventory Enrichment"
    ],
    "connector_count": 0,
    "group_order": 5
  },
  {
    "type": "GCP_CONNECTOR",
```

```
    "name": "GCP",
    "desc": "GCP Connector",
    "long_desc": "",
    "group": "Cloud",
    "index": 2,
    "appliance_type": "tetration_internal",
    "state": "disabled",
    "limit_per_appliance": 5000,
    "limit_per_rootscope": 5000,
    "limit_per_cluster": 100000,
    "config": [
      "GCP_CONNECTOR"
    ],
    "max_instances": 0,
    "noteworthy": true,
    "pre_release_tag": "BETA",
    "hidden": false,
    "capabilities": [
      "Managed K8s"
    ],
    "connector_count": 0,
    "group_order": 5
  }]
```

API pour supprimer un connecteur

Ce point terminal supprime le connecteur donné.

```
DELETE /openapi/v1/connectors/<id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur

Objet de réponse : renvoie l'état du connecteur supprimé.

Exemple de réponse

```
resp = restclient.delete('/connectors/63c12e316419d0131767e21c')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
 {
    "status": 200,
    "code": 1000,
    "message": "deleted"
  }
```

API pour obtenir un connecteur par ID

Ce point terminal obtient le connecteur à l'aide de l'ID donné.

```
GET /openapi/v1/connectors/<id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur

Objet de réponse : renvoie le connecteur à l'aide de l'ID donné.

Exemple de réponse

```
resp = restclient.get('/connectors/63c12e316419d0131767e21b')
 if resp.status_code == 200:
   parsed_resp = json.loads(resp.content)
   print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
   "name": "ERSPAN",
   "updated_at": 0,
   "created_at": 1673604657,
   "appliance_id": "63c1272039042a1c0ddd3e20",
   "root_scope_id": "63bf8d2f497d4f7287dbd335",
   "vrf_id": 1,
   "type": "ERSPAN",
   "ip_bindings": [],
   "internal": false,
   "id": "63c12e316419d0131767e21b"
 }
```

API pour renommer un connecteur

Ce point terminal renomme le connecteur à l'aide de l'ID donné.

```
PUT /openapi/v1/connectors/<id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
name	chaîne	Précisez le nouveau nom du connecteur

Objet de réponse : renvoie le connecteur avec l'ID et le nouveau nom donnés.

Exemple de réponse

```
req_payload = {
    "name": "ERSPAN2",
  }
  resp = restclient.put('/ext_appliances/63c12e316419d0131767e21b',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "name": "ERSPAN2",
    "updated_at": 0,
```

```
    "created_at": 1673604657,
    "appliance_id": "63c1272039042a1c0ddd3e20",
    "root_scope_id": "63bf8d2f497d4f7287dbd335",
    "vrf_id": 1,
    "type": "ERSPAN",
    "ip_bindings": [],
    "internal": false,
    "id": "63c12e316419d0131767e21b"
  }
```

API pour obtenir des renseignements sur le connecteur avec plus de détails

Ce point terminal obtient les informations sur le connecteur avec les détails.

```
GET /openapi/v1/connectors/cards/<type>?root_scope_id=<root_scope_id>
```

où <root_scope_id> est le root_scope_id qui peut être obtenu à partir de l'API Obtenir les portées, à la page 997. Dans la charge utile de la demande,<type> est une chaîne pour décider du type de connecteur.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Préciser la portée racine
type	chaîne	Précisez le type de connecteur. La valeur peut être « NETFLOW », « NETSCALER », « F5 » « AWS » « ANYCONNECT » « ASA » « SLACK » « KINESIS » « SYSLOG » « EMAIL » « MERAKI » « PAGERDUTY » « ISE » « SERVICENOW » « ERSPAN » « AWS_CONNECTOR » « AZURE_CONNECTOR » « GCP_CONNECTOR »

Objet de réponse : renvoie les connecteurs d'une portée donnée.

Exemple de réponse

```
resp = restclient.get('/connectors/cards/NETFLOW?root_scope_id=63bf8d2f497d4f7287dbd335')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "type": "NETFLOW",
    "name": "NetFlow",
    "desc": "Collect telemetry from network devices",
    "long_desc": "Collect NetFlow V9 and/or IPFIX telemetry from network devices such as
routers and switches.",
    "group": "Flow Ingest",
    "index": 0,
    "appliance_type": "tetration_data_ingest",
    "state": "disabled",
    "limit_per_appliance": 3,
    "limit_per_rootscope": 10,
```

```
    "limit_per_cluster": 100,
    "config": [
      "LOG",
      "ALERT"
    ],
    "max_instances": 0,
    "noteworthy": false,
    "hidden": false,
    "capabilities": [
      "Flow Visibility"
    ],
    "connector_count": 0,
    "info": {
      "help": "NetFlow connector collects telemetry data from various network devices (such
 as routers, switches).<br> It supports ingest of telemetry data in IPFIX and NetFlow V9
protocols. This connector can be used to discover inventory as it provides a network context.
 The connector helps convert data from flow exports and send them securely as Tetration
Flow records into an instance of Tetration. <br><br><b> Connector Alerts: </b><br> When
Connector Alerts are enabled, you may receive the following alerts: <br>   1. NetFlow
Connector is down (due to missing heartbeats). <br>   2. Informational alert on high
CPU/Memory usage."
    },
    "group_order": 0
  }
```


API pour obtenir des connecteurs

Ce point terminal renvoie tous les connecteurs pour un appareil donné.

```
GET
/openapi/v1/connectors?root_scope_id=<root_scope_id>&appliance_id=<appliance_id>&type=<type>&state=<state>
```

où <root_scope_id> est le root_scope_id qui peut être obtenu à partir de l'API Obtenir les portées, à la page 997, <appliance_id> est l'appareil_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127, <type> est une chaîne pour décider du type de connecteur qui peut être obtenue à partir du champ API pour obtenir le schéma de l'appareil, à la page 1137 « connecteurs », <state> est un filtre pour l'état des connecteurs.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
root_scope_id	chaîne	Préciser la portée racine
appliance_id	chaîne	Préciser l'ID de l'appareil
type	chaîne	Précisez le type de connecteur. La valeur peut être « NETFLOW », « NETSCALER » « F5 » « AWS » « ANYCONNECT » « ASA » « SLACK » « KINESIS » « SYSLOG » « EMAIL » « MERAKI » « PAGERDUTY » « ISE » « SERVICENOW » « ERSPAN » « AWS_CONNECTOR » « AZURE_CONNECTOR » « GCP_CONNECTOR »

Nom	Type	Description
state	chaîne	Filtrez l'état des connecteurs (la valeur peut être « ENABLED », « DISABLED » ou « UNAVAILABLE »)

Objet de réponse : renvoie tous les connecteurs pour un appareil donné.

Exemple de réponse

```
resp =
restclient.get('root_scope_id=63bf8d2f497d4f7287dbd335&appliance_id=63c1272039042a1c0ddd3e20&type=ERSPAN&state=ENABLED')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
[
    {
      "name": "ERSPAN",
      "updated_at": 0,
      "created_at": 1673604657,
      "appliance_id": "63c1272039042a1c0ddd3e20",
      "root_scope_id": "63bf8d2f497d4f7287dbd335",
      "vrf_id": 1,
      "type": "ERSPAN",
      "ip_bindings": [],
      "state": "enabled",
      "internal": false,
      "id": "63c12e316419d0131767e21b"
    },
    {
      "name": "ERSPAN",
      "updated_at": 0,
      "created_at": 1673604657,
      "appliance_id": "63c1272039042a1c0ddd3e20",
      "root_scope_id": "63bf8d2f497d4f7287dbd335",
      "vrf_id": 1,
      "type": "ERSPAN",
      "ip_bindings": [],
      "state": "enabled",
      "internal": false,
      "id": "63c12e316419d0131767e21c"
    },
    {
      "name": "ERSPAN",
      "updated_at": 0,
      "created_at": 1673604657,
      "appliance_id": "63c1272039042a1c0ddd3e20",
      "root_scope_id": "63bf8d2f497d4f7287dbd335",
      "vrf_id": 1,
      "type": "ERSPAN",
      "ip_bindings": [],
      "state": "enabled",
      "internal": false,
      "id": "63c12e316419d0131767e21d"
    }
  ]
```

API pour créer un connecteur

Ce point terminal crée un connecteur pour un appareil donné.

```
POST /openapi/v1/connectors
```

Dans la charge utile de la demande,<root_scope_id> est le root_scope_id qui peut être obtenu à partir de l'API Obtenir les portées, à la page 997,<appliance_id> est l'appliance_id qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127,<type> est une chaîne pour décider du type de connecteur qui peut être obtenue à partir du champ API pour obtenir le schéma de l'appareil, à la page 1137 « connecteurs ».

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Précisez le nom
root_scope_id	chaîne	Préciser la portée racine
appliance_id	chaîne	Préciser l'ID de l'appareil
type	chaîne	Précisez le type de connecteur. La valeur peut être « NETFLOW », « NETSCALER » « F5 » « AWS » « ANYCONNECT » « ASA » « SLACK » « KINESIS » « SYSLOG » « EMAIL » « MERAKI » « PAGERDUTY » « ISE » « SERVICENOW » « ERSPAN » « AWS_CONNECTOR » « AZURE_CONNECTOR » « GCP_CONNECTOR »
version	chaîne	Précisez la version

Objet de réponse : renvoie le connecteur créé.

Exemple de réponse

```
req_payload = {
    "root_scope_id": "63c41ff2497d4f5f5be73662",
    "appliance_id": "63c6ef42bca44e2b5e729191",
    "type": "NETFLOW",
    "name": "netflowtest",
    "version": "1.1.1"
  }
  resp = restclient.post('/connectors', json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "name": "netflowtest",
    "updated_at": 0,
    "created_at": 1674187875,
    "appliance_id": "63c6ef42bca44e2b5e729191",
    "root_scope_id": "63c41ff2497d4f5f5be73662",
```

```
    "vrf_id": 1,
    "type": "NETFLOW",
    "ip_bindings": [],
    "sources": [],
    "internal": false,
    "id": "63ca14631a49bd4c0e0cefa2"
  }
```


API pour obtenir les configurations sur le type de configuration du connecteur

Ce point terminal obtient les configurations du connecteur à l'aide de l'ID donné.

```
GET /openapi/v1/connectors/<id>/config?config_type=<config_type>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir la liste des appareils, à la page 1127. <config_type>est la « valid_config » qui peut être obtenue à partir de API pour obtenir le schéma de l'appareil, à la page 1137.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
config_type	chaîne	Précisez le type de configuration. Reportez-vous à API pour obtenir le schéma de configuration, à la page 1124 pour toutes les valeurs possibles répertoriées dans la description

Objet de réponse : renvoie les configurations avec l'ID de connecteur et le type de configuration donnés.

Exemple de réponse

```
resp = restclient.get('/connectors/63db5418e6ee1167a4c0986c/config?config_type=LOG')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
 [{
    "mode": "TEST_AND_APPLY",
    "name": "Log instance 2/1/23 22:29",
    "root_scope_id": "63d98f45497d4f53005b24fa",
    "vrf_id": 1,
    "appliance_id": "63dad690e6ee1131f255e985",
    "connector_id": "63db5418e6ee1167a4c0986c",
    "service_id": "63db5418e6ee1167a4c0986d",
    "deleted": false,
    "type": "LOG",
    "state": "COMMIT",
    "error_code": "NO_ERROR",
    "error_text": "",
    "attempts": 1,
    "config": {
      "secured": {},
      "unsecured": {
        "log-level": "info",
        "max-log-size": 10,
        "max-log-age": 30,
```

```
        "max-log-backups": 20
      }
    },
    "push_to_dio_at": 1675319360,
    "created_at": 1675319360,
    "updated_at": 1675319364,
    "discovery_completed_at": 0,
    "committed_at": 1675319364,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63db5840f029813659f9fcf5"
  }]
```

API pour ajouter une nouvelle configuration au connecteur

Ce point terminal ajoute une nouvelle configuration au connecteur à l'aide de l'ID donné

```
POST /openapi/v1/connectors/<id>/config
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153. <config_type>est la « valid_config » qui peut être obtenue à partir de API pour obtenir le schéma de l'appareil, à la page 1137. Pour obtenir<config> schéma, sélectionnez une des « config » de la réponse API pour obtenir tous les types de connecteurs, à la page 1142, appliquez la « config » à API pour obtenir le schéma de configuration, à la page 1124.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
name	chaîne	Préciser le nom de la configuration
type	chaîne	Précisez le type de configuration. Reportez-vous à API pour obtenir le schéma de configuration, à la page 1124 pour toutes les valeurs possibles répertoriées dans la description
config (configurer)	set	Fournir le schéma de configuration rempli au format JSON

Objet de réponse : renvoie la configuration mise à jour.

Exemple de réponse

```
req_payload = {
    "name": "Log instance 2/1/23 22:29",
    "type": "LOG",
    "config": {
      "secured": {},
      "unsecured": {
        "log-level": "info",
        "max-log-size": 10,
        "max-log-age": 30,
        "max-log-backups": 20
      }
    }
  }
```

```
  resp = restclient.post('/connectors/63db5418e6ee1167a4c0986c/config',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
{
    "mode": "TEST_AND_APPLY",
    "name": "Log instance 2/1/23 11:29",
    "root_scope_id": "63d98f45497d4f53005b24fa",
    "vrf_id": 1,
    "appliance_id": "63dad690e6ee1131f255e985",
    "connector_id": "63db5418e6ee1167a4c0986c",
    "deleted": false,
    "type": "LOG",
    "state": "PENDING",
    "attempts": 0,
    "config": {
      "secured": {},
      "unsecured": {
        "log-level": "info",
        "max-log-size": 10,
        "max-log-age": 30,
        "max-log-backups": 20
      }
    },
    "push_to_dio_at": 0,
    "created_at": 1675322272,
    "updated_at": 1675322272,
    "discovery_completed_at": 0,
    "committed_at": 0,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63db63a0f029813659f9fcf7"
  }
```


API pour supprimer une configuration

Ce point terminal supprime une configuration d'un connecteur donné.

```
DELETE /openapi/v1/connectors/<id>/config/<config_id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153, <config_id> est l'ID qui peut être obtenu à partir de API pour obtenir les configurations sur le type de configuration du connecteur, à la page 1156.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
config_id	chaîne	Préciser l'ID de configuration

Objet de réponse : renvoie l'état de la configuration supprimée pour un connecteur donné.

Exemple de réponse

```
resp =
restclient.delete('/connectors/63c1272039042a1c0ddd3e20/config/63c1272039042a1c0ddd3e21')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "status": 200,
    "code": 1000,
    "message": "deleted"
  }
```

-

API pour obtenir la configuration

Ce point terminal obtient la configuration à l'aide de l'ID donné

```
GET /openapi/v1/connectors/<id>/config/<config_id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153, <config_id> est l'ID qui peut être obtenu à partir de API pour obtenir les configurations sur le type de configuration du connecteur, à la page 1156.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID de l'appareil
config_id	chaîne	Préciser l'ID de configuration

Objet de réponse : renvoie la configuration à l'aide de l'ID donné.

Exemple de réponse

```
resp = restclient.get('/connectors/63db5418e6ee1167a4c0986c/config/63db5840f029813659f9fcf5')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "mode": "TEST_AND_APPLY",
    "name": "Log instance 2/1/23 22:29",
    "root_scope_id": "63d98f45497d4f53005b24fa",
    "vrf_id": 1,
    "appliance_id": "63dad690e6ee1131f255e985",
    "connector_id": "63db5418e6ee1167a4c0986c",
    "service_id": "63db5418e6ee1167a4c0986d",
    "deleted": false,
    "type": "LOG",
    "state": "COMMIT",
    "error_code": "NO_ERROR",
    "error_text": "",
    "attempts": 1,
    "config": {
      "secured": {},
      "unsecured": {
        "log-level": "info",
```

```
        "max-log-size": 10,
        "max-log-age": 30,
        "max-log-backups": 20
      }
    },
    "push_to_dio_at": 1675319360,
    "created_at": 1675319360,
    "updated_at": 1675319364,
    "discovery_completed_at": 0,
    "committed_at": 1675319364,
    "delete_at": 0,
    "error_at": 0,
    "hidden": false,
    "discovery_phase": 0,
    "internal": false,
    "id": "63db5840f029813659f9fcf5"
  }
```


API pour répertorier les commandes de dépannage disponibles pour le connecteur

Ce point terminal renvoie la liste des commandes de dépannage disponibles pour un connecteur donné.

```
GET /openapi/v1/connectors/<id>/commands/available
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur

Objet de réponse : renvoie la liste des commandes de dépannage disponibles pour un connecteur donné.

Exemple de réponse

```
resp = restclient.get('/connectors/63c6f2701a49bd2bb0696cab/commands/available')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse


```
[
    {
      "type": "LIST_SERVICE_FILES",
      "name": "List a directory in a service"
    },
    {
      "type": "CONTROLLER_PROFILING",
      "name": "Collect controller profile"
    },
    {
      "type": "SHOW_LOG",
      "name": "Show logs"
    },
    {
      "type": "SHOW_SERVICE_LOG",
      "name": "Show service logs"
    },
    {
      "type": "RESTART_CONNECTOR_CONTAINER",
      "name": "Restart the connector docker container"
    },
```

```
    {
      "type": "SHOW_SUPERVISOR_COMMANDS",
      "name": "Execute supervisorctl command"
    },
    {
      "type": "CONNECTOR_ALERT_INTERVAL_CONNECTOR",
      "name": "Override connector alert interval for Connector"
    },
    {
      "type": "SERVICE_PROFILING",
      "name": "Collect connector profile"
    },
    {
      "type": "SNAPSHOT_CONNECTOR",
      "name": "Collect Snapshot from a connector"
    },
    {
      "type": "PACKET_CAPTURE",
      "name": "Packet capture"
    },
    {
      "type": "NETWORK_CONNECTIVITY_COMMANDS",
      "name": "Test network connectivity"
    },
    {
      "type": "SHOW_SERVICE_RUNNING_CONF",
      "name": "Show running configuration of a service"
    },
    {
      "type": "RESTART_CONNECTOR_SERVICE",
      "name": "Restart the connector service"
    },
    {
      "type": "SHOW_SYS_COMMANDS",
      "name": "Execute system command"
    }
  ]
```


API pour lister toutes les commandes de dépannage

Ce point terminal renvoie la liste des commandes de dépannage activées pour un connecteur donné.

```
GET /openapi/v1/connectors/<id>/commands
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur

Objet de réponse : renvoie la liste des commandes de dépannage activées pour un connecteur donné.

Exemple de réponse

```
resp = restclient.get('/connectors/63db5418e6ee1167a4c0986c/commands')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
[
    {
      "appliance_id": "63dad690e6ee1131f255e985",
      "connector_id": "63db5418e6ee1167a4c0986c",
      "service_id": "63db5418e6ee1167a4c0986d",
      "state": "success",
      "level": "SERVICE",
      "command": "SHOW_LOG",
      "arg_string": "",
      "args": {
        "pattern": "info"
      },
      "tailed": false,
      "rc": 0,
      "push_to_dio_at": 1675319615,
      "attempts": 1,
      "error_code": "NO_ERROR",
      "error_text": "",
      "deleted": false,
      "deleted_at": 0,
      "created_at": 1675319613,
      "total_chunk": 0,
      "id": "63db593df029813659f9fcf6"
    }
  ]
```


API pour créer une commande de dépannage

Ce point terminal crée une commande de dépannage disponible pour un connecteur donné.

```
POST /openapi/v1/connectors/<id>/commands
```

ici<id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153. Dans la charge utile de la demande,<command> est un type de commande de dépannage qui peut être obtenu à partir de API pour répertorier les commandes de dépannage disponibles pour le connecteur, à la page 1160. <arguments>est un objet JSON contenant le schéma de commande, qui peut être obtenu à partir de API pour obtenir le schéma des commandes de dépannage, à la page 1125.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
commande	chaîne	Préciser le type de commande
arguments	set	Fournir le schéma de commande rempli au format JSON

Objet de réponse : renvoie la commande de dépannage créée pour l'appareil donné.

Exemple de réponse

```
req_payload = {
    "command": "SHOW_LOG",
    "arguments": {
      "pattern": "info"
    }
  }
  resp = restclient.post('/connectors/63db5418e6ee1167a4c0986c/commands',
json_body=json.dumps(req_payload))
  if resp.status_code == 200:
```

```
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "appliance_id": "63dad690e6ee1131f255e985",
    "connector_id": "63db5418e6ee1167a4c0986c",
    "service_id": "63db5418e6ee1167a4c0986d",
    "state": "pending",
    "level": "SERVICE",
    "command": "SHOW_LOG",
    "args": {
      "pattern": "info"
    },
    "tailed": false,
    "rc": 0,
    "push_to_dio_at": 0,
    "attempts": 0,
    "deleted": false,
    "deleted_at": 0,
    "created_at": 1675319613,
    "total_chunk": 0,
    "id": "63db593df029813659f9fcf6"
  }
```

API pour supprimer une commande de dépannage

Ce point terminal supprime une commande de dépannage disponible pour un connecteur donné.

```
DELETE /openapi/v1/connectors/<id>/commands/<command_id>
```

où <id> est un ID qui peut être obtenu à partir de la commande API pour obtenir des connecteurs, à la page 1153, <command_id> est l'ID qui peut être obtenu à partir de API pour lister toutes les commandes de dépannage, à la page 1139.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : renvoie l'état de la commande de dépannage supprimée pour le connecteur donné.

Exemple de réponse

```
resp =
restclient.delete('/connectors/63c12e316419d0131767e21c/commands/63c10a0039042a6aee1b008c')

  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "status": 200,
    "code": 1000,
    "message": "deleted"
  }
```

API pour renvoyer une commande de dépannage

Ce point terminal renvoie la commande de dépannage sélectionnée pour un connecteur donné.

```
GET /openapi/v1/connectors/<id>/commands/<command_id>
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153,<command_id> est l'ID qui peut être obtenu à partir de API pour lister toutes les commandes de dépannage, à la page 1139.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : renvoie la commande de dépannage sélectionnée pour un connecteur donné.

Exemple de réponse

```
resp =
restclient.get('/connectors/63db5418e6ee1167a4c0986c/commands/63db593df029813659f9fcf6')
  if resp.status_code == 200:
    parsed_resp = json.loads(resp.content)
    print json.dumps(parsed_resp)
```

Exemple de réponse

```
{
    "appliance_id": "63dad690e6ee1131f255e985",
    "connector_id": "63db5418e6ee1167a4c0986c",
    "service_id": "63db5418e6ee1167a4c0986d",
    "state": "success",
    "level": "SERVICE",
    "command": "SHOW_LOG",
    "arg_string": "",
    "args": {
      "pattern": "info"
    },
    "tailed": false,
    "rc": 0,
    "push_to_dio_at": 1675319615,
    "attempts": 1,
    "error_code": "NO_ERROR",
    "error_text": "",
    "deleted": false,
    "deleted_at": 0,
    "created_at": 1675319613,
    "total_chunk": 0,
    "id": "63db593df029813659f9fcf6"
  }
```

API pour télécharger la sortie de la commande du connecteur sous forme de fichier

Ce point terminal télécharge la sortie de la commande en tant que fichier.

```
GET /openapi/v1/connectors/<id>/commands/{command_id}/download
```

où <id> est l'ID qui peut être obtenu à partir de API pour obtenir des connecteurs, à la page 1153,<command_id> est l'ID qui peut être obtenu à partir de API pour lister toutes les commandes de dépannage, à la page 1139. Toutes les commandes n'ont pas une sortie téléchargeable, vérifiez le schéma de commande fourni par API

pour obtenir le schéma des commandes de dépannage, à la page 1125, où « output_type » : « FILE » indique qu'il a du contenu téléchargeable et « output_ext » indique le type de fichier.

Paramètres : L'URL de la demande contient les paramètres suivants :

Nom	Type	Description
ID	chaîne	Préciser l'ID du connecteur
command_id	chaîne	Préciser l'ID de commande

Objet de réponse : renvoie la commande de dépannage sélectionnée pour un connecteur donné.

Exemple de réponse

```
resp = restclient.download('downloadFile',
'/connectors/63c6ef42bca44e2b5e729191/commands/63cace941a49bd4c0e0cf45a/download')
```

CHAPITRE 19

Limites de configuration dans Cisco Secure Workload

Les limites des diverses fonctions de Cisco Secure Workload varient selon la version et la plateforme.

Flux et terminaux

Unité	Limite	8RU/39RU/SaaS/-
Nombre de serveurs simultanés (machine virtuelle ou sans système d'exploitation) à partir desquels les données de télémétrie peuvent être analysées par Cisco Secure Workload.	• Jusqu'à 10 000 avec télémétrie de flux détaillé Jusqu'à 20 000 avec télémétrie de flux de conversation uniquement	8RU
	• Jusqu'à 37 500 avec télémétrie de flux détaillé Jusqu'à 75 000 avec télémétrie de flux de conversation uniquement	39RU
Nombre d'événements de flux qui peuvent être traités par Cisco Secure Workload.	jusqu'à 500 000 par seconde	8RU
	jusqu'à 2 millions par seconde	39RU

Unité	Limite	8RU/39RU/SaaS/-
Nombre de flux activement suivis qui peuvent être traités par Cisco Secure Workload.	jusqu'à 10 000 000 par seconde	8RU
	jusqu'à 2 000 000 par seconde	39RU

Détenteurs, portées enfants, filtres d'inventaire et rôles

Unité	Limite	8RU/39RU
Nombre de charges de travail en mode de fidélité complète	10 000	8RU
	37 500	39RU
Nombre de détenteurs	7	8RU
	35	39RU
Nombre d'portées enfants par détenteur	1 000*	8RU
	5 000	39RU
Nombre d'portées enfants pour l'ensemble des détenteurs	7000	8RU
	35 000	39RU
nombre d'espaces de travail par détenteur	1 000*	8RU
	3 500*	39RU
Nombre d'espaces de travail pour tous les détenteurs	5 000	8RU
	20 000	39RU
nombre de filtres d'inventaire par détenteur	1 000*	8RU
	5 000*	39RU
Nombre de filtres d'inventaire pour tous les détenteurs	7 000*	8RU
	35 000*	39RU
Nombre de rôles par portée enfant	6	8RU
	6	39RU

Note * Si le mode conversation est activé sur tous les agents, Cisco Secure Workload prend en charge jusqu'à deux fois les limites mentionnées pour les limites marquées d'un astérisque (*). Pour en savoir plus, consultez Conversation Mode.

connecteurs infonuagiques

connecteurs infonuagiques	Unité	Limite	Évolutivité	Réseaux virtuels	Grappes Kubernetes
Connecteur AWS	Nombre total de flux exportés par le connecteur AWS	15 000 flux par seconde	5 comptes par connecteur	5 par compte	5 par compte
Connecteur Azure	Nombre total de flux exportés par le connecteur Azure	15 000 flux par seconde	5 abonnements par connecteur	5 par abonnement	5 par abonnement
Plateforme en nuage	Nombre total de flux exportés par le connecteur GCP	15 000 flux par seconde	5 projets par connecteur	5 par projet	5 par projet

Note

- Un maximum de 50 connecteurs, y compris les connecteurs infonuagiques, peuvent être configurés dans une grappe pour tous les détenteurs.
- Les charges de travail gérées par les connecteurs infonuagiques dans Cisco Secure Workload nécessitent des licences de charges de travail. Par conséquent, assurez-vous que le total de vos charges de travail est sous licence et dans les limites de la grappe.

Connecteurs

Note

- Un maximum de 50 connecteurs, y compris les connecteurs infonuagiques, peuvent être configurés dans une grappe pour tous les détenteurs.
- Pour connaître les limites applicables à chaque connecteur, consultez Que sont les connecteurs

Connecteur	Unité	Limite
Connecteur AnyConnect	Nombre total de points terminaux AnyConnect pris en charge par un connecteur AnyConnect	5000 points terminaux **Note** Le nombre de points terminaux AnyConnect sur tous les capteurs du serveur mandataire AnyConnect est limité par le nombre de capteurs pris en charge par l'appareil Cisco Secure Workload.
Connecteur AnyConnect	Nombre d'attributs LDAP qui pourraient être étiquetés dans les inventaires des points terminaux AnyConnect	6 attributs
Connecteur AWS	Nombre total de flux exportés par le connecteur AWS	15 000 flux par seconde
Connecteur F5	Nombre total de flux exportés par le connecteur F5	15 000 flux par seconde
Connecteur NetFlow	Nombre total de flux exportés par un connecteur NetFlow	15 000 flux par seconde
Connecteur NetScaler	Nombre total de flux exportés par le connecteur NetScaler	15 000 flux par seconde

Appliances virtuelles Cisco Secure Workload pour les connecteurs

Appareil	Unité	Limite
Dispositif d'acquisition Cisco Secure Workload	Nombre de connecteurs sur un appareil	3
	Nombre de périphériques par portée racine	100
	Nombre d'appareils par grappe	500
Appareil Cisco Secure Workload de périphérie	Nombre de connecteurs sur un appareil	6
	Nombre de périphériques par portée racine	1
	Nombre d'appareils par grappe	Nombre de portées racine

Limites des étiquettes

Fonctionnalités	Unité	Limite	8RU/39RU
Limites des étiquettes	Nombre maximal d'adresses IP qui peuvent être étiquetées pour toutes les portées racine	1 500 000 *	39RU
		500 000 *	8RU
	Nombre maximal de sous-réseaux qui peuvent être étiquetés dans toutes les portées racine	200 000	39RU
		50 000	8RU

Note * Lorsque le mode conversation est activé sur tous les agents, Cisco Secure Workload peut prendre en charge le double des limites mentionnées (limites marquées d'un astérisque (*)). Pour en savoir plus, consultez Conversation Mode.

Limites liées aux politiques

Fonctionnalités	Unité	Limite
Découverte automatique des politiques (anciennement ADM)	Nombre maximal de charges de travail des membres (terminaux) autorisées pour l'exécution de la découverte automatique des politiques sur une seule portée.	10 000
	Nombre maximal de conversations autorisées pour l'exécution de la découverte automatique des politiques sur une seule portée.	10 000 000
	Nombre maximal de charges de travail des membres (terminaux) autorisées pour la découverte automatique des politiques sur une branche de l'arborescence de portée.	37 500
	Nombre maximal de conversations autorisées pour la découverte automatique des politiques sur une branche de l'arborescence de la portée.	20 000 000
	Nombre maximal de charges de travail uniques (terminaux) autorisées pour l'exécution de la découverte automatique des politiques.	15 000 000
	Nombre maximal de filtres d'exclusion dans la configuration de découverte de politiques par défaut.	100
	Nombre maximal de filtres d'exclusion autorisés par espace de travail.	100
Politiques concrètes	La taille agrégée des politiques sur les agents installés sur des charges de travail autres que Kubernetes.	2,5 Mo (Environ 2 000 politiques, selon la complexité)
	La taille agrégée des politiques sur les agents installés sur les nœuds Kubernetes.	7,5 Mo (Environ 6 000 politiques, selon la complexité)

Fonctionnalités supplémentaires

Fonctionnalités	Unité	Limite
Alertes	Nombre d'instances prises en charge dans une portée racine	256
	Nombre d'instances prises en charge dans les portées racine	1024
	Nombre de dernières alertes affichées par portée racine (par catégorie d'état – ACTIVE (ACTIVE), SNOOZED (RÉPÉTÉE), MUTED (EN SOURDINE), CLOSED (FERMÉE))	5 000
	Taux d'alerte maximal à prévisualiser dans l'interface utilisateur	60 par minute. **Note** Si plus de 60 alertes sont envoyées par minute, l'interface utilisateur affiche un message récapitulatif indiquant que des alertes ont été envoyées aux enregistreurs de données mais qu'elles sont supprimées de l'interface utilisateur. Notez que les 60 alertes par minute s'appliquent à la fréquence à laquelle les alertes sont envoyées aux dérivations de données, et ne s'appliquent pas à l'heure, ni à l'événement d'alerte et n'est pas lié à un lot spécifique de données.
	Nombre d'alertes configurées par portée racine (boîte de dialogue modale)	1 000

Fonctionnalités	Unité	Limite
	Nombre maximal d'alertes traitées par l'application Alertes par lot par minute	20 000
Application Compliance (Conformité)	Nombre d'espaces de travail pris en charge	128

Fonctionnalités	Unité	Limite	8RU/39RU/-
Nombre d'éléments de l'inventaire suivis	Nombre maximal d'adresses IP qui peuvent être suivies pour toutes les portées racine	1 500 000 *	39RU
		500 000 *	8RU
	Nombre maximal de sous-réseaux qui peuvent être suivis pour toutes les portées racine	200 000	39RU
		50 000	8RU

Données entrantes ou sortantes

Fonctionnalités	Unité	Limite	8RU/39RU/SaaS/-
Dérivations de données	Nombre de dérivations de données prises en charge par appareil	10	-

CHAPITRE 20

Cisco Secure Workload Virtual (SECURE-WORKLOAD-V)

Secure Workload Virtual

Instructions for deploying Cisco Secure Workload Virtual (formerly known as Tetration-V) are available from https://www.cisco.com/c/en/us/support/security/tetration-analytics-g1/model.html

CHAPITRE 21

Contrat de licence de l'utilisateur final

End User License Agreement

To view the End User License Agreement and Supplemental End User License Agreement for your product, go to https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Click the **Supplemental End User License Agreements** tab and search for your product.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.