Guide de démarrage rapide Cisco Secure Workload, version 3.8

Première publication : 2023-04-12

À propos de ce guide

Ce document s'applique à la version 3.8 de Cisco Secure Workload :

- Il présente les concepts clés de Cisco Secure Workload : la segmentation, les étiquettes de charge de travail, les potées, les arborescences hiérarchiques de portées et la découverte des politiques.
- Il explique le processus de création de la première branche de votre arborescence de portée à l'aide de l'assistant de première expérience utilisateur.
- Il décrit le processus automatisé de génération de politiques pour l'application choisie en fonction des flux de trafic réels.

Introduction

En règle générale, la sécurité des réseaux vise à empêcher les activités malveillantes de pénétrer dans le réseau à l'aide de pare-feu installés à la périphérie de ce dernier. Cependant, vous devez également protéger votre entreprise contre les menaces qui ont atteint votre réseau ou qui proviennent de celui-ci. La segmentation (ou microsegmentation) du réseau permet de protéger les charges de travail en contrôlant le trafic entre celles-ci et les autres hôtes du réseau; ainsi, seul le trafic nécessaire à l'activité de l'entreprise est autorisé et tout autre trafic est refusé.

Par exemple, vous pouvez utiliser des politiques pour empêcher toute communication entre les charges de travail qui hébergent votre application Web publique et la base de données de recherche et développement de votre centre de données, ou pour empêcher les charges de travail hors production d'entrer en contact avec les charges de travail de production.

Cisco Secure Workload utilise les données de flux de l'entreprise pour proposer des politiques que vous pouvez évaluer et approuver avant de les appliquer. Vous pouvez également créer manuellement ces politiques pour segmenter votre réseau.

Visite de l'assistant

Bienvenue dans Cisco Secure Workload. L'étiquetage et le regroupement de vos charges de travail sont essentiels pour tirer parti de la puissance de Cisco Secure Workload.

L'intégration est une approche conviviale et guidée qui vous aide à configurer et à déployer des applications en toute sécurité dans votre environnement. Vous pouvez segmenter votre réseau pour autoriser uniquement le trafic nécessaire à votre entreprise et bloquer toutes les autres communications.

Pour vous aider à démarrer, choisissez Aperçu dans le menu de gauche pour accéder à l'assistant de démarrage rapide. L'assistant prépare généralement Cisco Secure Workload à démarrer la création de politiques de

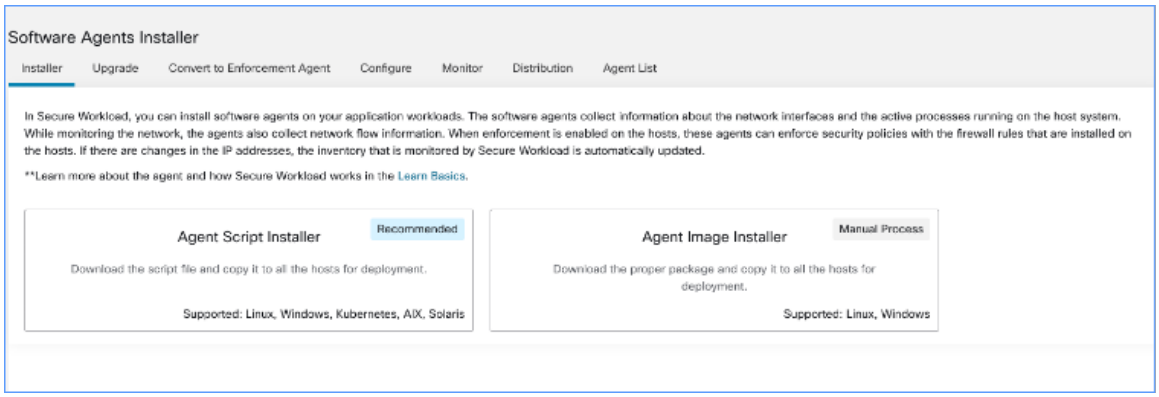
segmentation pour contrôler le trafic sur votre réseau, présente une série d'étapes, chacune se concentrant sur un aspect spécifique de la sécurité, et invite les utilisateurs à faire des choix en connaissance de cause pour configurer leur charge de travail de manière sécurisée.

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

- L'administrateur de site
- Le service d'assistance à la clientèle
- Le propriétaire de la portée

Installer les agents

Cisco Secure Workload vous permet d'installer des agents logiciels sur vos charges de travail applicatives. Les agents logiciels recueillent des renseignements sur les interfaces réseau et les processus actifs sur le système hôte.



Vous pouvez installer les agents logiciels de deux manières :

- Programme d'installation du script d'agent : utilisez cette méthode pour l'installation, le suivi et le dépannage des problèmes lors de l'installation des agents logiciels. Les plateformes prises en charge sont Linux, Windows, Kubernetes, AIX et Solaris
- Programme d'installation de l'image de l'agent : téléchargez l'image de l'agent logiciel pour installer une version et un type d'agent logiciel précis pour votre plateforme. Les plateformes prises en charge sont Linux et Windows.

L'assistant d'intégration vous guide dans le processus d'installation des agents en fonction de la méthode d'installation sélectionnée. Consultez les instructions d'installation sur l'interface utilisateur et le guide de l'utilisateur pour en savoir plus sur l'installation des agents logiciels.

Regrouper et étiqueter vos charges de travail

Attribuez des étiquettes à un groupe de charges de travail pour créer une portée. L'arborescence hiérarchique de la portée permet de diviser les charges de travail en groupes plus restreints. La branche inférieure de l'arborescence de la portée est réservée aux applications individuelles.

Sélectionnez une portée parente dans l'arborescence des portées pour créer une nouvelle portée, qui contient un sous-ensemble des membres de la portée parente.

Dans cette fenêtre, vous pouvez organiser vos charges de travail en groupes, qui sont classés selon une structure hiérarchique. La division de votre réseau en groupes hiérarchiques permet une découverte et une définition de politiques flexibles et évolutives.

Les étiquettes sont des paramètres clés qui décrivent une charge de travail ou point terminal. Ces éléments sont représentés sous forme d'une paire clé-valeur. L'assistant vous aide à appliquer les étiquettes à vos charges de travail, puis regroupe ces étiquettes en groupes appelés portées. Les charges de travail sont automatiquement regroupées en portées en fonction de leurs étiquettes associées. Vous pouvez définir des politiques de segmentation en fonction des portées.

Passez le curseur sur chaque bloc ou chaque portée dans l'arborescence pour obtenir plus de renseignements sur le type de charges de travail ou d'hôtes qu'il ou elle comprend.

Remarque Dans la fenêtre Get Started with Scopes and Labels (Démarrer avec les portées et les étiquettes), Organisation, Infrastructure, Environnement et Application sont les légendes, et le texte des cases grises en ligne avec chaque légende sont les valeurs.

Par exemple, toutes les charges de travail appartenant à l'application 1 sont définies par l'ensemble d'étiquettes suivant :

- Organisation = interne
- Infrastructure = Centres de données
- Environnement = Pré-production
- Application = Application 1

La puissance des étiquettes et des arborescences de portée

Les étiquettes sont le moteur de la puissance de Cisco Secure Workload, et l'arborescence de portée créée à partir de vos étiquettes est bien plus qu'un simple résumé de votre réseau :

- Les étiquettes vous permettent de comprendre instantanément vos politiques :

  ```
  "Deny all traffic from Pre-Production to Production"
  ```

  Comparez ceci à la même politique sans étiquette :

  ```
  "Deny all traffic from 172.16.0.0/12 to 192.168.0.0/16"
  ```

- Les politiques basées sur des étiquettes s'appliquent automatiquement (ou cessent de s'appliquer) lorsque des charges de travail étiquetées sont ajoutées à l'inventaire (ou supprimées de ce dernier). Au fil du temps, ces regroupements dynamiques basés sur des étiquettes réduisent considérablement le travail d'entretien de votre déploiement.
- Les charges de travail sont regroupées en portées en fonction de leurs étiquettes. Ces regroupements vous permettent d'appliquer facilement une politique aux charges de travail connexes. Par exemple, vous pouvez facilement appliquer une politique à toutes les applications de la portée Pré-production.
- Les politiques créées une seule fois dans une seule portée peuvent être automatiquement appliquées à toutes les charges de travail des portées subordonnées dans l'arborescence, ce qui minimise le nombre de politiques à gérer.

  Vous pouvez facilement définir et appliquer une politique générale (par exemple, à toutes les charges de travail de votre entreprise) ou restreinte (aux seules charges de travail qui font partie d'une application

spécifique) ou à n'importe quel niveau intermédiaire (par exemple, à toutes les charges de travail de votre centre de données).

- Vous pouvez attribuer la responsabilité de chaque portée à différents administrateurs, en déléguant la gestion des politiques aux personnes qui connaissent le mieux chaque partie de votre réseau.

Établir la hiérarchie pour votre entreprise

Commencez à construire votre hiérarchie ou arborescence de portée, ce qui implique d'identifier et de classer les ressources, de déterminer la portée, de définir les rôles et les responsabilités, d'élaborer des politiques et des procédures pour créer une branche de l'arborescence de la portée.

L'assistant vous guide dans la création d'une branche de l'arborescence de la portée. Saisissez des adresses IP ou des sous-réseaux pour chaque portée à contour bleu. Les étiquettes sont automatiquement appliquées en fonction de l'arborescence de la portée.

Prérequis :

- Regroupez les adresses IP et les sous-réseaux associés à votre environnement de pré-production, à vos centres de données et à votre réseau interne.
- Collectez autant d'adresses IP/de sous-réseaux que vous pouvez, vous pourrez ajouter des adresses IP/des sous-réseaux supplémentaires ultérieurement.
- Ultérieurement au fur et à mesure que vous créez votre arborescence, vous pourrez ajouter des adresses IP/des sous-réseaux pour les autres portées de l'arborescence (les blocs gris).

Pour créer l'arborescence de portée, procédez comme suit :

Définir la portée interne

La portée interne comprend toutes les adresses IP qui définissent le réseau interne de votre entreprise, y compris les adresses IP publiques et privées.

L'assistant vous guide dans l'ajout d'adresses IP à chaque portée de la branche de l'arborescence. Au fur et à mesure que vous ajoutez des adresses, l'assistant attribue des étiquettes à chaque adresse qui définit la portée.

Par exemple, dans cette fenêtre de configuration de portée, l'assistant attribue l'étiquette

`Organization=Internal`

à chaque adresse IP.

Par défaut, l'assistant ajoute les adresses IP dans l'espace d'adresses Internet privée comme défini dans la RFC 1918

Remarque Toutes les adresses IP n'ont pas à être saisies en même temps, mais vous devez inclure les adresses IP associées à l'application de votre choix. Vous pouvez ajouter les autres adresses IP ultérieurement.

Définir la portée du centre de données

Cette portée comprend les adresses IP qui définissent vos centres de données sur site. Saisissez les adresses IP et les sous-réseaux qui définissent votre réseau interne.

Remarque Les noms de portée doivent être courts et significatifs.

Dans cette fenêtre, indiquez les adresses IP que vous avez saisies pour l'entreprise. Ces adresses doivent être un sous-ensemble des adresses de votre réseau interne. Si vous possédez plusieurs centres de données, incluez-les tous dans cette portée pour pouvoir définir un seul ensemble de politiques.

Remarque Vous pourrez toujours ajouter d'autres adresses ultérieurement. Par exemple, l'assistant attribue ces étiquettes à chacune des adresses IP :

```
Organization=Internal
Infrastructure=Data Centers
```

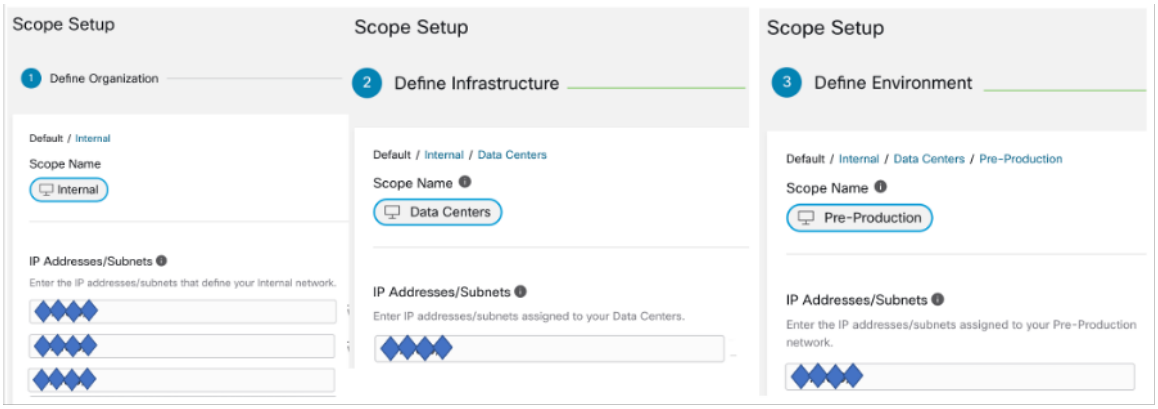
Définir la portée de pré-production

Cette portée comprend les adresses IP des applications et des hôtes hors production, tels que les systèmes de développement, de laboratoire, de test ou de préparation.

Remarque Veillez à ne pas inclure les adresses des applications utilisées pour mener des activités commerciales réelles; utilisez-les pour la portée de production que vous définirez ultérieurement.

Les adresses IP que vous saisissez dans cette fenêtre doivent être un sous-ensemble des adresses que vous avez saisies pour vos centres de données, y compris les adresses de l'application que vous avez choisie. Idéalement, elles devraient également inclure les adresses de pré-production qui ne font pas partie de l'application choisie.

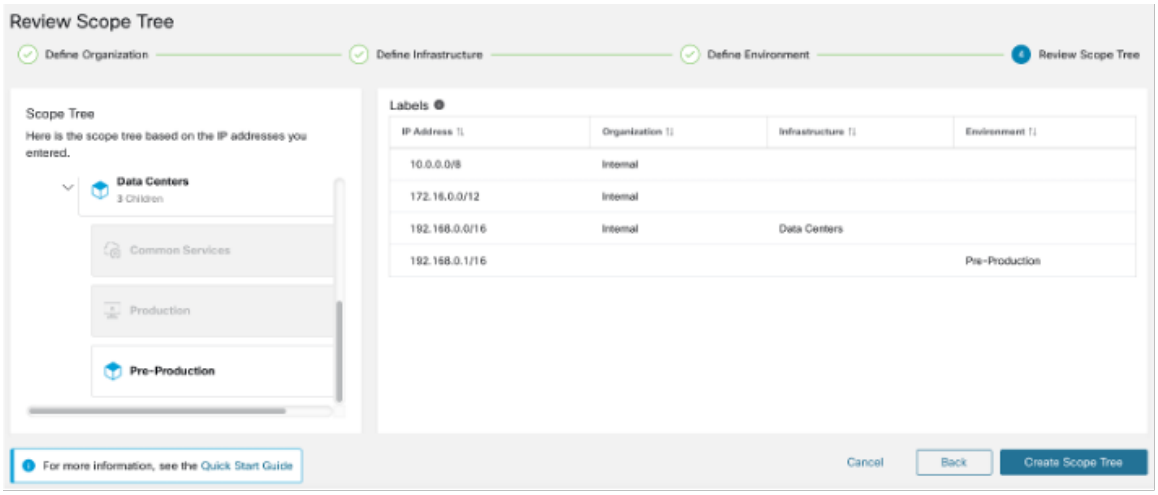
Remarque Vous pourrez toujours ajouter d'autres adresses ultérieurement.



Examinez l’arborescence des portées, les portées et les étiquettes.

Avant de commencer à créer l’arborescence de la portée, examinez la hiérarchie que vous pouvez voir dans la fenêtre de gauche. La portée racine affiche les étiquettes qui ont été créées automatiquement pour toutes les adresses IP configurées et tous les sous-réseaux. À une étape ultérieure du processus, les applications sont ajoutées à cette arborescence de portée.

Illustration 1 :

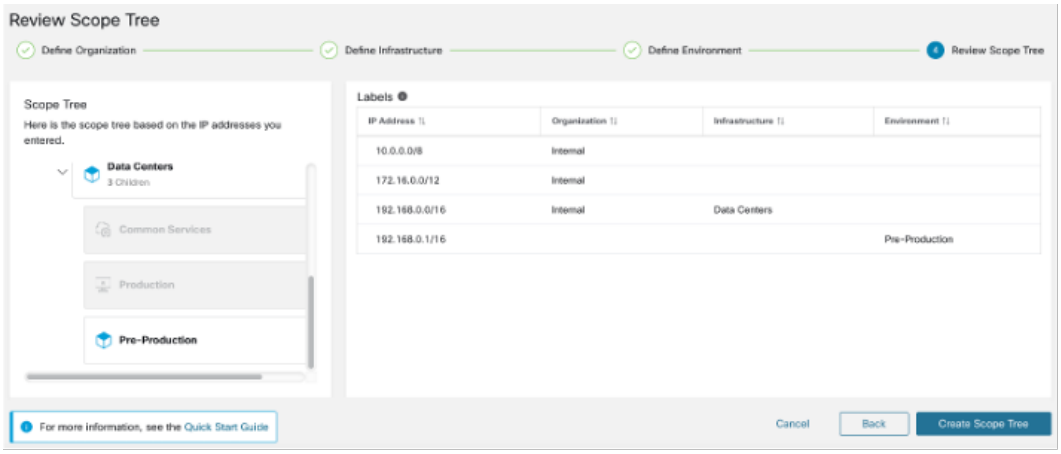


Vous pouvez développer et réduire les branches de l'arborescence et faire défiler la liste vers le bas pour choisir une portée spécifique. Dans le volet droit, vous pouvez afficher les adresses IP et les étiquettes attribuées aux charges de travail pour la portée spécifique. Dans cette fenêtre, vous pouvez passer en revue et modifier l’arborescence de la portée avant d’ajouter une application à cette dernière.

Remarque Si vous souhaitez afficher ces informations après avoir quitté l’assistant, choisissez Organize (Organiser) > Scopes (Portées) et Inventory (inventaire) dans le menu principal.

Examiner l'arborescence de la portée

Avant de commencer à créer l’arborescence de la portée, examinez la hiérarchie que vous pouvez voir dans la fenêtre de gauche. La portée racine affiche les étiquettes qui ont été créées automatiquement pour toutes les adresses IP configurées et tous les sous-réseaux. À une étape ultérieure du processus, les applications sont ajoutées à cette arborescence de portée.

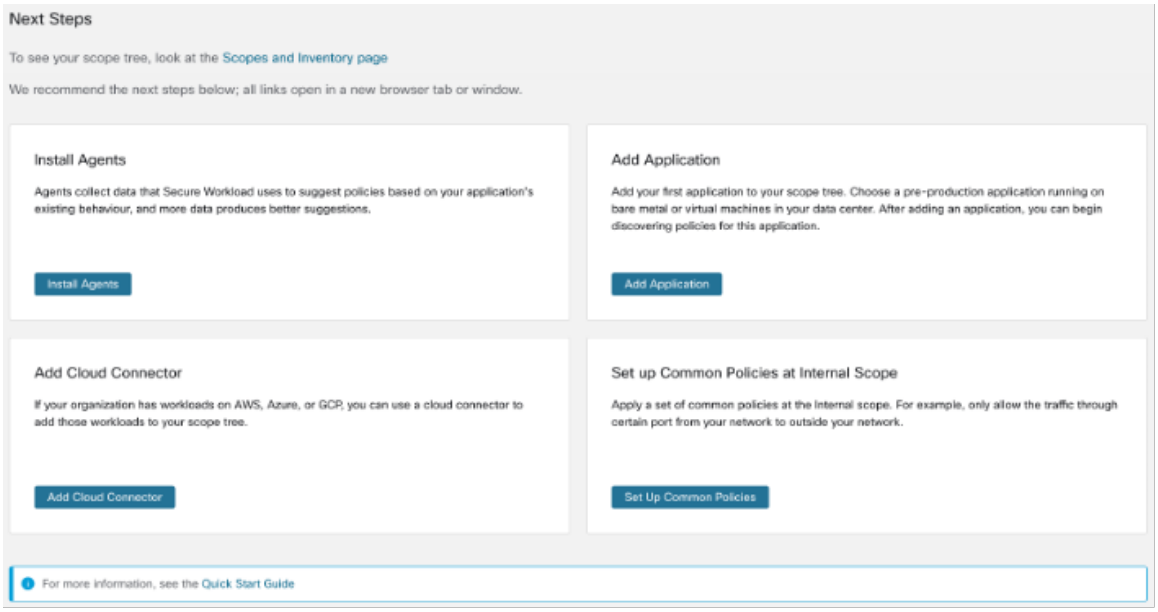


Vous pouvez développer et réduire les branches de l'arborescence et faire défiler la liste vers le bas pour choisir une portée spécifique. Dans le volet droit, vous pouvez afficher les adresses IP et les étiquettes attribuées aux charges de travail pour la portée spécifique. Dans cette fenêtre, vous pouvez examiner et modifier l'arborescence de la portée avant d'ajouter une application à cette dernière.

Remarque Si vous souhaitez afficher ces informations après avoir quitté l'assistant, choisissez **Organize (Organiser)** > **Scopes (Portées)** et **Inventory (inventaire)** dans le menu principal.

Créer une arborescence de portée

Après avoir passée en revue l'arborescence de portée, créez-la.



Pour en savoir plus sur l'arborescence de portée, consultez les sections Portées et Inventaire dans le guide de l'utilisateur.

Prochaines étapes

Installer les agents

Installez les agents Cisco Secure Workload sur les charges de travail associées à l'application choisie. Les données recueillies par les agents sont utilisées pour suggérer des politiques basées sur le trafic existant sur votre réseau. Plus les données sont nombreuses, plus les politiques produites sont précises. Pour en savoir plus, consultez la section Agents logiciels dans le guide de l'utilisateur de Cisco Secure Workload.

Ajout d'une application

Ajoutez la première application à votre arborescence. Choisissez une application de pré-production fonctionnant sur des machines sans système d'exploitation ou sur des machines virtuelles dans votre centre de données. Après avoir ajouté une application, vous pouvez commencer la découverte des politiques pour cette application. Pour en savoir plus, consultez la section sur la portée et l'inventaire du guide de l'utilisateur de Cisco Secure Workload.

Configurer les politiques communes au niveau de la portée interne

Appliquer un ensemble de politiques communes au niveau de la portée interne Par exemple, n'autoriser que le trafic passant par certains ports de votre réseau vers l'extérieur de celui-ci.

Les utilisateurs peuvent définir des politiques manuellement à l'aide des grappes, des filtres d'inventaire et des portées, ou celles-ci peuvent être découvertes et générées à partir des données de flux à l'aide d'une découverte automatique des politiques.

Après avoir installé les agents et laissé les données de trafic se cumuler pendant au moins quelques heures, vous pouvez permettre à Cisco Secure Workload de générer (« découvrir ») des politiques basées sur ce trafic. Pour en savoir plus, consultez la section sur la découverte automatique des politiques du guide de l'utilisateur de Cisco Secure Workload.

Appliquez ces politiques à la portée interne (aussi dénommée intérieure ou racine) pour examiner efficacement les politiques.

Ajouter un Cloud Connector

Si votre entreprise dispose de charges de travail sur AWS, Azure ou GCP, utilisez un Cloud Connector (Connecteur infonuagique) pour ajouter ces charges de travail à votre arborescence de portée. Pour en savoir plus, consultez la section Cloud Connectors du guide de l'utilisateur de Cisco Secure Workload.

Flux de travail de démarrage rapide

Étape	Faire ceci	Détails
1	(Facultatif) Effectuer une visite commentée de l'assistant	Visite de l'assistant, à la page 1
2	Choisir une application pour commencer votre parcours de segmentation.	Pour de meilleurs résultats, suivez les instructions figurant dans Choisisir une application pour cet assistant, à la page 9.
3	Recueillir des adresses IP.	L'assistant nécessitera quatre groupes d'adresses IP. Pour de plus amples renseignements, consultez la section Recueillir des adresses IP, à la page 9.

Étape	Faire ceci	Détails
4	Exécuter l'assistant	Pour afficher les exigences et accéder à l'assistant, consultez Exécuter l'assistant, à la page 10.
5	Laisser aux agents le temps de recueillir des données sur les flux.	Plus les données sont nombreuses, plus les politiques produites sont précises. Le temps minimal nécessaire dépend du niveau d'utilisation de votre application.
6	Générer (« Découvrir ») des politiques en fonction de vos données de flux réelles.	Consultez Générer automatiquement des politiques, à la page 11.

Recueillir des adresses IP

Vous aurez besoin d'au moins quelques-unes des adresses IP mentionnées à chaque point ci-dessous :

- Les adresses qui définissent votre réseau interne

  Par défaut, l'assistant utilise les adresses standard réservées pour une utilisation privée d'Internet.

- Les adresses réservées à vos centres de données.

  Cela n'inclut pas les adresses utilisées par les ordinateurs des employés, les services infonuagiques ou de partenaires, les services d'informatique centralisée, etc.

- Les adresses qui définissent votre réseau hors production
- Les adresses des charges de travail qui composent l'application hors production de votre choix

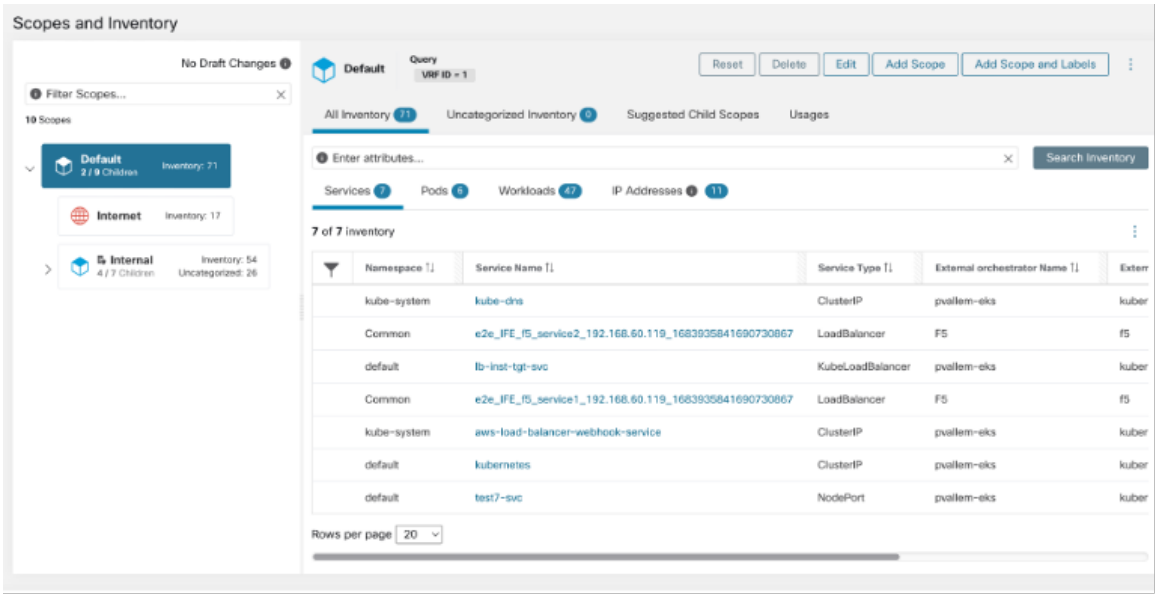
Pour l'instant, il n'est pas nécessaire d'avoir toutes les adresses correspondant à chacun des points ci-dessus; vous pourrez toujours en ajouter ultérieurement.

Important Étant donné que chacun des quatre points représente un sous-ensemble des adresses IP du point qui le précède, il est nécessaire que chaque adresse IP de chaque point soit également incluse dans les adresses IP du point qui le précède dans la liste.

Choisisir une application pour cet assistant

Pour cet assistant, choisissez une seule application.

Une application se compose généralement de plusieurs charges de travail qui fournissent différents services, tels que des services Web ou des bases de données, des serveurs primaires et de secours, etc. Ces charges de travail fournissent collectivement la fonctionnalité de l'application à leurs utilisateurs.



Directives pour le choix de votre application

Cisco Secure Workload prend en charge les charges de travail s'exécutant sur un large éventail de plateformes et de systèmes d'exploitation, y compris les charges de travail infonuagique et en conteneurs. Cependant, dan le cadre de cet assistant, choisissez une application avec des charges de travail qui sont :

- En cours d'exécution dans votre centre de données.
- Fonctionnent sur des machines sans système d'exploitation et/ou des machines virtuelles.
- Fonctionnant sur les plateformes Windows, Linux ou AIX prises en charge par les agents Cisco Secure Workload, consultez la page https://www.cisco.com/go/secure-workload/requirements/agents.
- Déployées vers un environnement de production,

Remarque Vous pouvez exécuter l'assistant même si vous n'avez pas choisi d'application ni rassemblé d'adresses IP, mais vous ne pouvez pas achever son exécution sans avoir effectué ces opérations.

Remarque Si vous ne terminez pas l'exécution de l'assistant avant de vous déconnecter (ou de vous interrompre en cas d'expiration du délai) ou si vous naviguez vers une autre partie de l'application Cisco Secure Workload (utilisez la barre de navigation de gauche), les configurations de l'assistant ne sont pas sauvegardées.

Pour plus de détails sur la façon d'ajouter une portée seule, une portée et des étiquettes, consultez la section Portées et inventaire du Guide de l'utilisateur de Cisco Secure Workload.

Exécuter l'assistant

Vous pouvez exécuter l'assistant que vous ayez ou non choisi une application et collecté des adresses IP, mais vous ne pourrez pas terminer son exécution si vous n'avez pas effectué ces opérations.

Important Si vous ne terminez pas les opérations de l'assistant avant de vous déconnecter (ou avant l'expiration du délai) de Cisco Secure Workload, ou si vous passez à une partie différente de l'application en utilisant la barre de navigation de gauche, les configurations de l'assistant ne sont pas enregistrées.

Avant de commencer

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

- administrateur du site
- Le service d'assistance à la clientèle
- Le propriétaire de la portée

Procédure

Étape 1 Se connecter à Cisco Secure Workload.

Étape 2 Démarrez l'assistant.

Si aucune portée n'est actuellement définie, l'assistant s'affiche automatiquement lorsque vous vous connectez à Cisco Secure Workload.

Vous pouvez aussi faire comme suit :

- Cliquez sur le lien **Run the wizard now** (Exécuter l'assistant maintenant) dans la bannière bleue en haut d'une page quelconque.
- Choisissez **Overview** (Aperçu) dans le menu principal sur le côté gauche de la fenêtre.

Si vous avez déjà créé des portées, vous ne pouvez pas accéder à nouveau à l'assistant à moins de supprimer toutes les portées existantes. Pour ce faire, (Facultatif) Réinitialiser l'arborescence de la portée., à la page 12.

Étape 3 L'assistant vous explique ce que vous devez savoir.

Ne négligez pas les éléments utiles suivants :

- Passez la souris sur les éléments graphiques de l'assistant pour lire leur description.
- Cliquez sur les liens et les boutons d'information (Bouton d'information) pour obtenir des renseignements importants.

Générer automatiquement des politiques

Cisco Secure Workload génère et détecte des politiques en fonction du trafic existant entre les charges de travail et d'autres hôtes. Vous pouvez modifier, compléter, analyser et éventuellement approuver et appliquer les politiques sur les charges de travail.

Avant de commencer

- Installer les agents sur les charges de travail de votre application

- Après l'installation de l'agent, il faut attendre un certain temps pour que les données de flux s'accumulent.

Procédure

Étape 1 Sur la page **Next Steps** (prochaines étapes) de l'assistant de démarrage rapide, cliquez sur **Automatically Generate Policies** (Générer automatiquement des politiques).

Sinon, vous pouvez effectuer les opérations suivantes :

a) Choisissez **Défend > Segmentation** (Défendre > Segmentation) dans la barre de menus de gauche.
b) Dans le volet gauche, dans l'arborescence ou la liste des portées, faites défiler la liste jusqu'à la portée de l'application.
c) Choisissez **Primary** (Principale) dans cette portée.

Étape 2 Choisissez **Manage Policies** (gestion des politiques).

Étape 3 Choisissez **Automatically Discover Policies** (Découvrir automatiquement les politiques) .

Étape 4 Choisissez la plage temporelle des données de flux que vous souhaitez inclure :

Étape 5 Choisissez **Discover Policies** (Découvrir les politiques). Les politiques générées s'affichent sur cette page.

(Facultatif) Réinitialiser l'arborescence de la portée.

Vous pouvez supprimer les portées, les étiquettes et l'arborescence des portées que vous avez créées à l'aide de l'assistant et exécuter l'assistant à nouveau (facultatif).

Astuces Si vous ne souhaitez supprimer que certaines des portées créées et ne pas réexécuter l'assistant, supprimez des portées individuelles au lieu de réinitialiser toute l'arborescence des portées. Pour supprimer une portée, choisissez Portée et cliquez sur **Delete** (Supprimer).

Avant de commencer

Il faut disposer des privilèges du propriétaire de la portée pour la portée racine.

Si vous avez créé des espaces de travail, des politiques ou d'autres dépendances supplémentaires, consultez le guide de l'utilisateur de Cisco Secure Workload pour obtenir des renseignements complets sur la réinitialisation de l'arborescence de la portée.

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 le bouton Reset (réinitialiser) passe à Pending Reset (En attente de réinitialisation), vous devrez peut-être actualiser la page du navigateur.

Autres renseignements

Pour en savoir plus sur les concepts de l'assistant, consultez le guide de l'utilisateur de Cisco Secure Workload.

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.