Guide de mise à niveau Cisco Secure Workload

Première publication : 2021-10-29

Dernière modification : 2024-05-15

Chemins de mise à niveau pris en charge pour Cisco Secure Workload

Tableau 1 : Chemins de mise à niveau pris en charge pour Cisco Secure Workload

De	Vers	Type de mise à niveau
3.9.1.1	3.9.1.10	Mise à niveau des correctifs
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.9.1.1	Mise à niveau de la version principale
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.44	Mise à niveau des correctifs
3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.39	Mise à niveau des correctifs
3.8.1.19 3.8.1.1	3.8.1.36	Mise à niveau des correctifs
3.8.1.1	3.8.1.19	Mise à niveau des correctifs
3.7.1.59 3.7.1.51 3.7.1.39	3.8.1.1	Mise à niveau de la version principale
3.7.1.51 3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.59	Mise à niveau des correctifs

De	Vers	Type de mise à niveau
3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.51	Mise à niveau des correctifs
3.7.1.22 3.7.1.5	3.7.1.39	Mise à niveau des correctifs
3.7.1.5	3.7.1.22	Mise à niveau des correctifs
3.6.x	3.7.1.5	Mise à niveau de la version principale
3.6.1.x	Tout correctif 3.6 ultérieur	Mise à niveau des correctifs
3.5.1.x (Marque Tetration)	3.6.1.5	Mise à niveau de la version principale
Les versions antérieures à la 3.6.	Toute version antérieure à la 3.6. Pour en savoir plus sur les spécificités , consultez le *Guide de mise à niveau de Cisco Tetration,* disponible ici.	–

Exigences et limites du mode double pile (prise en charge d'IPv6)

Les grappes de Cisco Secure Workload exécutées sur du matériel physique peuvent être configurées pour utiliser IPv6 en plus d'IPv4 pour certaines communications à destination et à partir de la grappe.

Remarque

- Vous pouvez utiliser la fonctionnalité en mode Double pile (prise en charge IPv6) lors de l'installation ou de la mise à niveau vers les versions 3.6.1.5, 3.7.1.5, 3.8.1.1 et 3.9.1.1. Toutefois, l'option permettant d'activer la fonctionnalité n'est pas disponible lors de l'installation ou de la mise à niveau des versions correctives.
- Les agents communiquent avec la grappe à l'aide d'IPv4, sauf si vous les configurez pour utiliser IPv6. Pour en savoir plus, consultez le guide de l'utilisateur Cisco Secure Workload.

Restrictions

Si vous envisagez d'activer le mode double pile, tenez compte des éléments suivants :

- Vous ne pouvez activer la connectivité IPv6 que lors du déploiement initial ou de la mise à niveau vers une version majeure (vous ne pouvez pas activer cette fonctionnalité lors des mises à niveau des correctifs).
- Le mode double pile est pris en charge uniquement sur le matériel physique ou les grappes sans système d'exploitation.
- Le mode IPv6 uniquement n'est pas pris en charge.

- Vous ne pouvez pas revenir au mode IPv4 uniquement après l'activation du mode double pile sur la grappe.
- (Applicable aux versions 3.8 et antérieures) La sauvegarde et la restauration des données (DBR) ne sont pas prises en charge si la connectivité double pile est activée.
- N'activez pas le mode double pile pour les grappes configurées avec la Fédération.
- Les fonctionnalités suivantes utilisent toujours et uniquement IPv4 (notez qu'IPv4 est toujours activé, même si IPv6 est activé) :
  - (Applicable aux versions 3.9.1.1, 3.8.1.1, 3.7.1.5 et 3.6.x) Application sur les agents AIX
  - (Applicable uniquement à la version 3.6.x) Communication de l'agent matériel avec la grappe
  - (Applicables uniquement à la version 3.6.x) Connecteurs pour l'acquisition de flux, l'enrichissement de l'inventaire ou les notifications d'alertes

Exigences

- Configurez les enregistrements DNS A et AAAA pour le nom de domaine complet avant d'activer le mode double pile pour votre grappe.
- Les services externes tels que NTP, SMTP et DNS doivent être disponibles sur IPv4 et IPv6, à des fins de redondance.
- Pour configurer le mode double pile pour une grappe :
  - Chacun des deux commutateurs à ressort à lame de la grappe doit se voir attribuer des adresses IPv6 routables sur deux réseaux différents, à des fins de redondance, et des passerelles par défaut doivent être fournies pour chaque réseau.
  - Pour les grappes 39RU, un réseau IPv6 routable sur site avec de l'espace pour au moins 29 adresses d'hôte est requis.
  - Pour les grappes 8RU, un réseau IPv6 routable sur site avec de l'espace pour au moins 20 adresses d'hôte est requis.
  - Les trois premières adresses d'hôte du réseau IPv6 routable de site sont réservées pour la configuration HSRP de la grappe Cisco Secure Workload et ne doivent pas être utilisées par d'autres périphériques.

Mise à niveau vers la version Cisco Secure Workload 3.9.x

Mise à niveau vers la version Cisco Secure Workload 3.9.1.10

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.9.1.1.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.10.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.9.1.10-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau de **service d'assistance à la clientèle** possède une clé SSH qui est chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans le volet de navigation, choisissez **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mise à niveau/redémarrage/arrêt).

Étape 3 Suivez les instructions à l'écran.

Dépannez tous les problèmes identifiés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le lien **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration Cisco Secure Workload.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Sélectionnez le correctif RPM téléchargé et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lance la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface utilisateur et afficher les résultats de la mise à niveau.

En cas de problème avec la mise à niveau, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.
b) Dans le volet de navigation, cliquez sur **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau est réussie, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à niveau des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.9.1.1

Vous pouvez effectuer une mise à niveau vers cette version à partir de n'importe quelle version 3.8. Cependant, nous vous recommandons d'effectuer la mise à niveau vers la dernière version corrigée 3.8.1.x avant de procéder à la mise à niveau vers cette version.

Avant de commencer

⚠

Mise en garde N'effectuez pas la mise à niveau si l'un des nœuds est mis hors service ou si l'un des services n'est pas intègre. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Orchestrateurs externes de Kubernetes AKS : après la mise à niveau, les orchestrateurs externes AKS seront en lecture seule; si vous souhaitez apporter des modifications après la mise à niveau, créez un nouveau connecteur Azure et activez l'option **Managed Kubernetes services** (Services gérés Kubernetes).
- Orchestrateurs externes FMC : Après la mise à niveau, les orchestrateurs externes FMC sont migrés vers les connecteurs.
- Assurez-vous qu'un compte de niveau de *service d'assistance à la clientèle* possède une clé SSH qui est chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.
- Si des connecteurs ISE sont configurés, vérifiez que leurs certificats TLS comportent des sections Subject Alternative Name (SAN). Après la mise à niveau, le connecteur ISE ne se connectera pas aux terminaux ISE qui présentent d'anciens certificats TLS CN uniquement. Ne procédez pas à la mise à niveau avant que les certificats ISE TLS ne soient régénérés avec les extensions SAN.
- **Licence**

- Si votre déploiement Cisco Secure Workload ne comporte pas de licences Cisco Smart valides (ou s'il est en dehors de la période d'évaluation), vous devez enregistrer des licences valides avant d'effectuer la mise à niveau.
- Des privilèges d'administrateur de site sont nécessaires pour gérer les licences.
- Pour afficher l'état de vos licences : Dans l'interface utilisateur de Cisco Secure Workload, sélectionnez **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Licenses (Licences)** . Si l'enregistrement de votre licence de grappe n'est pas conforme, une bannière s'affichera sur l'interface utilisateur. Pour savoir comment obtenir et enregistrer des licences, dans l'interface utilisateur Cisco Secure Workload, sélectionnez **Help (Aide)** > **Page-Level help)(Aide au niveau de la page)** et recherchez Smart Licensing.

Procédure

Étape 1 Accédez à la page https://software.cisco.com/download/home/286309796/type et téléchargez les fichiers RPM applicables à votre déploiement.

- Pour un système 8 RU ou 39 RU, téléchargez les fichiers RPM suivants :
  - tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.9.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
- Pour un système virtuel, téléchargez les RPM suivants :
  - tetration_os_ova_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-5.el6.x86_64.rpm

Étape 2 Vérifiez que la somme de contrôle MD5 des fichiers RPM téléchargés correspond à la somme de contrôle MD5 sur Cisco.com.

Étape 3 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 4 Un instantané de la grappe aide à résoudre les problèmes liés à la mise à niveau. Dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Snapshots (Instantanés)** > **Create Snapshots(Créer des instantanés)** > **Classic Snapshots (Instantanés classiques)**.

a) Ne modifiez pas les paramètres par défaut.
b) Dans le champ **Comments** (Commentaires), saisissez un commentaire pour l'instantané.
c) Cliquez sur **Create Snapshot** (Créer un instantané).

Étape 5 Dans le volet de navigation, choisissez **Platform(Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**.

Étape 6 Sous l'onglet **Upgrade** (mise à niveau), suivez les instructions qui s'affichent à l'écran. Veillez à ne sauter aucune étape.

Remarque Sous **Select Operation**(sélectionner une opération), choisissez **Upgrade** (Mise à niveau) pour cette mise à niveau. *Ne choisissez pas l'option de mise à niveau des correctifs*.

Étape 7 Cliquez sur **Envoyer le lien de mise à niveau**.

L'administrateur du site ou l'utilisateur du service d'assistance à la clientèle connecté recevra un courriel avec pour objet :

```
[Tetration Analytics] Upgrade Initiation Link
```

Étape 8 Cliquez sur le lien figurant dans le courriel. Sinon, vous pouvez récupérer l'URL de mise à niveau en cliquant sur **Troubleshoot (Dépannage)** > **Maintenance Explorer** (Explorateur d'entretien) et en saisissant les renseignements suivants :

- Action sur l'instantané :**POST**
- Hôte de l'instantané :**orchestrator.service.consul**
- Chemin de l'instantané :**upgrade_url**

Remarque Google Chrome et Microsoft Edge sont les navigateurs Web pris en charge pour cette mise à niveau.

Le portail de configuration de Cisco Secure Workload s'affiche.

Étape 9 Dans le portail de configuration de Cisco Secure Workload, téléchargez les fichiers RPM.

a) Cliquez sur **Choose file** (Choisir le fichier).
b) Naviguez et sélectionnez *tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm*, puis cliquez sur **Open** (Ouvrir).
c) Cliquez sur **Upload** (Téléverser).
d) Une fois le fichier *tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm* téléchargé avec succès, cliquez sur **Install** (Installer).
Une fois le fichier *tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm* installé, les fichiers RPM dépendants sont chargés et ces fichiers RPM peuvent être déployés pour le déploiement. Vous pouvez afficher les versions du fichier RPM actuellement déployé et du fichier RPM mis à disposition.
e) Répétez les étapes **a** à **c** pour les fichiers RPM dépendants en fonction de votre déploiement de grappe. Reportez-vous à l'étape 1 pour obtenir la liste des fichiers RPM.

La liste des fichiers RPM sur la page ne se met pas à jour au fur et à mesure que vous les téléchargez, ce qui est normal. Si vous constatez une erreur après le chargement du fichier *tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm*, attendez 5 à 10 minutes, puis rechargez la page. Vous devriez maintenant pouvoir afficher la liste des RPM téléchargés.

Remarque Si vous effectuez une mise à niveau vers cette version à partir de la version 3.8.1.1, téléchargez les fichiers RPM dans l'ordre suivant. Après avoir téléchargé le fichier *tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm*, la page s'actualise et vous remarquerez que les fichiers RPM téléchargés sont transférés. Vous pouvez maintenant charger les autres fichiers RPM.

- Pour un système 8 RU ou 39 RU :
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  - tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
- Pour un système virtuel :
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm

Les lignes qui sont surlignées en vert indiquent que les fichiers RPM sont chargés avec succès. En cas de problème, cliquez sur **Status** (État) pour afficher le journal.

Étape 10 Cliquez sur **Install** (Installer) pour déployer les fichiers RPM.

Étape 11 Cliquez sur **Continue** (Continuer).
Le portail **Site Config** 'Configuration du site) s'affiche.

Remarque À partir de la version 3.8 de Cisco Secure Workload et des versions ultérieures, les caractères non ASCII ne peuvent être saisis dans les champs de texte relatifs aux configurations de site à l'aide de l'interface utilisateur d'installation de Cisco Secure Workload.

Étape 12 (Facultatif) Sous **General** (Général), modifiez la clé publique SSH et cliquez sur **Next** (Suivant).

Étape 13 (Facultatif) Sous **Email** (Adresse de courriel), modifiez l'administrateur de l'interface utilisateur ou l'adresse de courriel de l'administrateur, puis cliquez sur **Next** (Suivant).

Étape 14 (Facultatif) Sous **L3**, autorisez la grappe à utiliser des adresses IPv6 en plus des adresse IPv4 pour certaines connectivités de la grappe après la mise à niveau. Pour activer IPv6 :

a) Cochez la case **IPv6**.
b) Saisissez les adresses IPv6 en notation CIDR pour les commutateurs à ressort à lame 1 et 2.
c) Saisissez la passerelle par défaut IPv6 du commutateur à ressort à lame1 et ressort à lame2.
d) Cliquez sur **Next** (suivant).

Si vous activez IPv6 sur cette page, vous devez également configurer les champs IPv6 sur la page **Network** (Réseau), décrite à l'étape suivante.

Important Pour les exigences et les limites du mode pile double, consultez Exigences et limites du mode double pile (prise en charge d'IPv6), à la page 2.

Étape 15 Sous **Network** (Réseau) :

a) Au besoin, modifiez les valeurs de **CIMC Internal Network (Réseau interne CIMC)**, de **CIMC Internal Network Gateway (Passerelle réseau interne CIMC)**, de **DNS Resolve (Résolveur DNS)** et de **DNS Domain (Domaine DNS).**

b) **Important** Ne modifiez, ni ne supprimez la valeur **External Network** (Réseau externe) existante.

Cependant, vous pouvez ajouter d'autres réseaux IPv4.

c) Si vous avez activé IPv6 à la page L3, la case **IPv6** est automatiquement cochée. Préciser les adresses IPv6 qui sont réservées pour une utilisation de Cisco Secure Workload par :

1. Saisissez le réseau externe IPv6 en notation CIDR.
2. (Facultatif) Pour utiliser l'adresse IPv6 uniquement pour des adresses spécifiées, saisissez les adresses IP IPv6 externes individuelles.

Remarque
- Les trois premières adresses IPv6 dans le champ Réseau externe IPv6 sont toujours réservées pour les commutateurs de la grappe Cisco Secure Workload et ne doivent pas être utilisées à d'autres fins.
- Pour une grappe 39 RU, vérifiez qu'au moins 29 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.
- Pour une grappe 8 RU, vérifiez qu'au moins 20 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.

d) Cliquez sur **Next** (suivant).

Étape 16 (Facultatif) Sous **Service** (Service), modifiez les valeurs NTP et SMTP, puis cliquez sur **Next** (Suivant).

Étape 17 Sous **Security**(sécurité), activez ou désactivez les chiffrements SSL renforcés pour les connexions des agents, puis cliquez sur **Next**(suivant).

Vous ne pouvez pas modifier les valeurs sous les onglets **UI** (Interface utilisateur), **Advanced** (Avancé) et **Recovery** (Récupération).

Sous **Recovery** (Récupération), si la grappe est configurée pour être une grappe de secours, elle est déployée en mode veille, ce qui inclut des fonctionnalités réduites (uniquement pour prendre en charge le mode veille à chaud).

Étape 18 Cliquez sur **Continue** (Continuer).
Les vérifications suivantes sont effectuées au cours du processus de mise à niveau pour s'assurer que :

- Les versions RPM sont correctes.
- La grappe est intègre.
- Les renseignements sur le site que vous avez fournis sont valides.
- Les commutateurs sont configurés correctement et peuvent être mis à niveau vers une version plus récente du logiciel NX-OS.
- Les champs de renseignements sont validés
- Le protocole NTP est synchronisé avant le début du déploiement.

- Le nœud de nom et de nom secondaire ne sont pas dans un état de basculement

Les vérifications peuvent prendre de quelques minutes à une heure si les commutateurs de la grappe doivent être mis à niveau. Une fois les vérifications terminées, vous recevrez un courriel avec pour objet : `TETRATION CLUSTER MyCluster: Verify Token` (GRAPPE TETRATION MaGrappe : Jeton de vérification). Le message contient un jeton dont vous aurez besoin pour continuer la mise à niveau. Copiez le jeton de ce courriel.

Étape 19 Dans le portail de configuration de Cisco Secure Workload, collez le jeton dans le champ **Validation Token** (jeton de validation) et cliquez sur **Continue**(continuer) .

Important Ne cochez pas la case **Ignore instance stop failures** (Ignorer les échecs d'arrêt de l'instance), à moins que l'assistance technique Cisco TAC ne vous le demande expressément.

Le processus de mise à niveau est lancé. Dans les versions 3.9.1.1, 3.8.1.1 et 3.7.1.5, les machines virtuelles de l'orchestrateur seront mises à niveau avant les autres composants. Cela peut prendre de 30 à 60 minutes, pendant lesquels la barre de progression passe de 0 à 100 %. Une fois les mises à niveau des orchestrateurs terminées, les autres composants seront mis à niveau et la barre de progression recommencera à 0 %. Lorsque la barre de progression verte atteint 100 %, la mise à niveau est terminée. Toutes les instances affichent l'état *Deployed* (Déployé).

Étape 20 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.
b) Dans le volet de navigation, choisissez **Platform (Plateforme) > Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt).**
c) Cliquez sur **History** (Historique).
d) Vérifiez que l'état dans la colonne **Status** (État) est **Succeeded** (Réussite).

Prochaine étape

Après la mise à niveau, apportez les modifications nécessaires pour bénéficier des améliorations de cette version :

- Si vous avez activé IPv6, vous pouvez accéder à l'interface utilisateur de Cisco Secure Workload en utilisant une adresse IPv4 ou IPv6. Par défaut, les agents continuent de se connecter à la grappe à l'aide d'IPv4. Si vous souhaitez que les agents logiciels puissent communiquer avec la grappe à l'aide d'IPv6 :

  1. Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)**.
  2. Configurez le paramètre **Sensor VIP FQDN** (Nom de domaine complet VIP du capteur) comme décrit dans le Guide de l'utilisateur Cisco Secure Workload.

- Pour la mise en grappe améliorée des charges de travail standard de Kubernetes dans les portées, reportez vous à Mises à niveau vers les versions 3.9, 3.8 et 3.7 : activation de la mise en grappe améliorée des charges de travail Kubernetes dans la découverte de politiques, à la page 32.

Mise à niveau vers la version Cisco Secure Workload 3.8.x

Mise à niveau vers la version Cisco Secure Workload 3.8.1.39

Vous pouvez effectuer une mise à niveau vers cette version à partir des versions 3.8.1.1, 3.8.1.19 ou 3.8.1.36.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.39.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.8.1.39-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau de **service d'assistance à la clientèle** possède une clé SSH qui est chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans le volet de navigation, choisissez **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mise à niveau/redémarrage/arrêt).

Étape 3 Suivez les instructions à l'écran.

Dépannez tous les problèmes identifiés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le lien **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration Cisco Secure Workload.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Sélectionnez le correctif RPM téléchargé et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lance la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface utilisateur et afficher les résultats de la mise à niveau.

En cas de problème avec la mise à niveau, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.
b) Dans le volet de navigation, cliquez sur **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau est réussie, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à niveau des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.8.1.36

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.8.1.1 ou 3.8.1.19.

Avant de commencer

⚠

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.36.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.8.1.36-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau de **service d'assistance à la clientèle** possède une clé SSH qui est chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans le volet de navigation, choisissez **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mise à niveau/redémarrage/arrêt).

Étape 3 Suivez les instructions à l'écran.

Dépannez tous les problèmes identifiés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le lien **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration Cisco Secure Workload.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Sélectionnez le correctif RPM téléchargé et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lance la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface utilisateur et afficher les résultats de la mise à niveau.

En cas de problème avec la mise à niveau, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.

b) Dans le volet de navigation, cliquez sur **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).

c) Cliquez sur **History** (Historique).

d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau est réussie, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à niveau des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.8.1.19

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.8.1.1.

Avant de commencer

⚠

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.19.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.8.1.19-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau de **service d'assistance à la clientèle** possède une clé SSH qui est chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans le volet de navigation, choisissez **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mise à niveau/redémarrage/arrêt).

Étape 3 Suivez les instructions à l'écran.

Dépannez tous les problèmes identifiés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le lien **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration Cisco Secure Workload.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Sélectionnez le correctif RPM téléchargé et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lance la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface utilisateur et afficher les résultats de la mise à niveau.

En cas de problème avec la mise à niveau, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.
b) Dans le volet de navigation, cliquez sur **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau est réussie, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à niveau des correctifs).

Mise à niveau vers la version 3.8.1.1 de Cisco Secure Workload

Vous devez effectuer une mise à niveau vers la dernière version corrigée 3.7.1.x avant de procéder à la mise à niveau vers cette version.

Avant de commencer

⚠

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

Gardez ces points à l'esprit :

- Orchestrateurs externes de Kubernetes AKS : après la mise à niveau, les orchestrateurs externes AKS seront en lecture seule; si vous souhaitez apporter des modifications après la mise à niveau, créez un nouveau connecteur Azure et activez l'option **Managed Kubernetes services** (Services gérés Kubernetes).

- Orchestrateurs externes FMC : Après la mise à niveau, les orchestrateurs externes FMC sont migrés vers les connecteurs.
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome et Microsoft Edge sont les navigateurs pris en charge pour la mise à niveau.
- Si des connecteurs ISE sont configurés, vérifiez que leurs certificats TLS comportent des sections Subject Alternative Name (SAN). Après la mise à niveau, le connecteur ISE ne se connectera pas aux terminaux ISE qui présentent d'anciens certificats TLS CN uniquement. Ne procédez pas à la mise à niveau avant que les certificats ISE TLS ne soient régénérés avec les extensions SAN.
- **Licence**
  - Si votre déploiement Cisco Secure Workload ne dispose pas actuellement de licences Smart Cisco valides (ou est en dehors de la période d'évaluation), vous devez enregistrer des licences valides avant de procéder à la mise à niveau.
  - Des privilèges d'administrateur de site sont nécessaires pour gérer les licences.
  - Pour afficher l'état de vos licences : Dans le portail Web Cisco Secure Workload, sélectionnez **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Licenses (Licences)**. Si l'enregistrement de votre licence de grappe n'est pas conforme, vous verrez une bannière s'afficher sur l'interface utilisateur. Pour savoir comment obtenir et enregistrer des licences, dans le portail Web Cisco Secure Workload, sélectionnez **Help (Aide)** > **Page-Level help (Aide au niveau de la page)** et recherchez Smart Licensing.

Procédure

Étape 1 Téléchargez les fichiers RPM applicables à votre déploiement à partir de Cisco.com :

a) Accédez à https://software.cisco.com/download/home/286309796/type.

b) Téléchargez le cas échéant :

- Pour un système 8-RU ou 39-RU, téléchargez les RPM suivants :
  - tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.8.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- Pour un système virtuel, téléchargez les RPM suivants :

- tetration_os_ova_k9-3.8.1.1-1.noarch.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_enforcement_k9-3.8.1.1-5.el6.x86_64.rpm

c) Vérifiez que la somme de contrôle MD5 des RPM téléchargés correspond à la somme de contrôle MD5 dans CCO.

Étape 2 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Sur l'interface utilisateur Cisco Secure Workload, dans le volet de navigation, choisissez **Troubleshoot (Dépannage)** > **Service Status (État du service).**

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All**(développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 3 Dans le volet de navigation de gauche, choisissez **Platform (Plateforme)** > **Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt)**.

Étape 4 Sous l'onglet **Upgrade** (mise à niveau), suivez les instructions qui s'affichent à l'écran. Veillez à ne sauter aucune étape.

Remarque Sous **Select Operation**(sélectionner une opération), choisissez **Upgrade**(mise à niveau). NE choisissez PAS l'option de mise à niveau des correctifs.

Étape 5 Cliquez sur **Envoyer le lien de mise à niveau**.

Un utilisateur connecté avec un rôle d'administrateur de site ou de service d'assistance à la clientèle recevra un courriel avec un lien hypertexte qui devra être utilisé pour effectuer la mise à niveau. L'objet du courriel sera :

```
[Tetration Analytics] Upgrade Initiation Link
```

Ouvrez le courriel et copiez l'URL **Upgrade Cluster** (Mise à niveau de la grappe).

Sinon, vous pouvez récupérer l'URL de mise à niveau en cliquant sur **Troubleshoot(Dépannage)** > **Maintenance Explorer** (Explorateur d'entretien) et en saisissant les renseignements suivants :

- Action sur l'instantané :**POST**
- Hôte de l'instantané :**orchestrator.service.consul**
- Chemin de l'instantané :**upgrade_url**

Étape 6 Dans le navigateur, collez l'URL de mise à niveau dans le champ d'adresse et appuyez sur la touche **Entrée**.

Le portail de configuration de Cisco Secure Workload s'affiche. Notez que Google Chrome et Microsoft Edge sont les navigateurs Web pris en charge pour la mise à niveau.

Étape 7 Dans le portail de configuration de Cisco Secure Workload, vous devez charger les fichiers RPM dans un ordre spécifique selon votre configuration. Pour charger les fichiers RPM, procédez comme suit :

a) Cliquez sur **Choose file** (Choisir le fichier).
b) Naviguez jusqu'à un fichier RPM, sélectionnez-le, puis cliquez sur **Open** (Ouvrir).
c) Cliquez sur **Upload** (Téléverser).
d) Répétez les étapes **a** à **c** pour chaque fichier RPM.
La liste des fichiers RPM sur la page ne se met pas à jour au fur et à mesure que vous les téléchargez, ce qui est normal. Si vous constatez une erreur après le chargement du fichier *tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm*, attendez 5 à 10 minutes, puis rechargez la page. Vous devriez maintenant pouvoir afficher la liste des RPM téléchargés.

Pour un système 8-RU ou 39-RU, chargez les fichiers suivants dans l'ordre indiqué :

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.3.8.1.1-1.el7.x86_64.rpm

Pour un système virtuel, chargez les fichiers suivants dans l'ordre indiqué :

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.8.1.1-1.noarch.rpm

Étape 8 Cliquez sur **Continue** (Continuer).
Le portail **Site Config** 'Configuration du site) s'affiche.

Remarque À partir des versions 3.8 et ultérieures de Cisco Secure Workload, les caractères non ASCII ne peuvent être saisis dans les champs de texte relatifs aux configurations de site à l'aide de l'interface utilisateur de configuration de Cisco Secure Workload.

Étape 9 (Facultatif) Sous **General** (Général), modifiez la clé publique SSH et cliquez sur **Next** (Suivant).

Étape 10 (Facultatif) Sous **Email** (Adresse de courriel), modifiez l'administrateur de l'interface utilisateur ou l'adresse de courriel de l'administrateur, puis cliquez sur **Next** (Suivant).

Étape 11 (Facultatif) Sous **L3**, autorisez la grappe à utiliser des adresses IPv6 en plus des adresse IPv4 pour certaines connectivités de la grappe après la mise à niveau. Pour activer IPv6 :

a) Cochez la case **IPv6**.
b) Saisissez les adresses IPv6 en notation CIDR pour les commutateurs à ressort à lame 1 et 2.
c) Saisissez la passerelle par défaut IPv6 du commutateur à ressort à lame1 et ressort à lame2.
d) Cliquez sur **Next** (suivant).

Si vous activez IPv6 sur cette page, vous devez également configurer les champs IPv6 sur la page **Network** (Réseau), décrite à l'étape suivante.

Important Pour les exigences et les limites du mode pile double, consultez Exigences et limites du mode double pile (prise en charge d'IPv6), à la page 2.

Étape 12 Sous **Network** (Réseau) :

a) Au besoin, modifiez les valeurs de **CIMC Internal Network (Réseau interne CIMC)**, de **CIMC Internal Network Gateway (Passerelle réseau interne CIMC)**, de **DNS Resolve (Résolveur DNS)** et de **DNS Domain (Domaine DNS).**

b) **Important!** Ne modifiez, ni ne supprimez la valeur **External Network** (Réseau externe) existante. Cependant, vous pouvez ajouter des réseaux IPv4 supplémentaires.

c) Si vous avez activé IPv6 à la page L3, la case **IPv6** est automatiquement cochée. Préciser les adresses IPv6 réservées pour une utilisation de Cisco Secure Workload par :

1. Saisissez le réseau externe IPv6 en notation CIDR.
2. (Facultatif) Pour utiliser l'adresse IPv6 uniquement pour des adresses spécifiées, saisissez les adresses IP IPv6 externes individuelles.

Remarque
- Les trois premières adresses IPv6 dans le champ Réseau externe IPv6 sont toujours réservées pour les commutateurs de la grappe Cisco Secure Workload et ne doivent pas être utilisées à d'autres fins.
- Pour une grappe 39 RU, vérifiez qu'au moins 29 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.
- Pour une grappe 8 RU, vérifiez qu'au moins 20 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.

d) Cliquez sur **Next** (suivant).

Étape 13 (Facultatif) Sous **Service** (Service), modifiez les valeurs NTP et SMTP, puis cliquez sur **Next** (Suivant).

Étape 14 Sous **Security**(sécurité), activez ou désactivez les chiffrements SSL renforcés pour les connexions des agents, puis cliquez sur **Next**(suivant).

Vous ne pouvez pas modifier les valeurs sous les onglets **UI** (Interface utilisateur), **Advanced** (Avancé) et **Recovery** (Récupération).

Sous **Recovery** (Récupération), si la grappe est configurée pour être une grappe de secours, elle sera déployée en mode veille, ce qui inclut des fonctionnalités réduites (uniquement pour prendre en charge le mode veille à chaud).

Étape 15 Cliquez sur **Continue** (Continuer).
Les vérifications suivantes sont effectuées au cours du processus de mise à niveau pour s'assurer que :

- Les versions RPM sont correctes
- La grappe est intègre
- Les renseignements sur le site que vous avez fournis sont valides
- Les commutateurs sont configurés correctement et peuvent être mis à niveau vers une version plus récente du logiciel NX-OS
- Les champs de renseignements sont validés

- Le protocole NTP est synchronisé avant le début du déploiement
- Le nœud de nom et de nom secondaire ne sont pas dans un état de basculement

Les vérifications peuvent prendre de quelques minutes à une heure si les commutateurs de la grappe doivent être mis à niveau. Une fois les vérifications terminées, vous recevrez un courriel avec pour objet : `TETRATION CLUSTER MyCluster: Verify Token` (GRAPPE TETRATION MaGrappe : Jeton de vérification). Le message contient un jeton dont vous aurez besoin pour continuer la mise à niveau. Copiez le jeton de ce courriel.

Étape 16 Dans le portail de configuration de Cisco Secure Workload, collez le jeton dans le champ **Validation Token** (jeton de validation) et cliquez sur **Continue**(continuer) .

Important Ne cochez pas la case **Ignore instance stop failures** (Ignorer les échecs d'arrêt de l'instance), à moins qu'un collaborateur de Cisco ne vous le demande expressément.

Le processus de mise à niveau est lancé. Dans les versions 3.8.1.1 et 3.7.1.5, les machines virtuelles de l'orchestrateur seront mises à niveau avant les autres composants. Cela peut prendre de 30 à 60 minutes, pendant lesquels la barre de progression passera de 0 à 100 %. Une fois les mises à niveau des orchestrateurs terminées, les autres composants seront mis à niveau et la barre de progression recommencera à 0 %. Lorsque la barre de progression verte atteint 100 %, la mise à niveau est terminée. Toutes les instances affichent l'état « Deployed » (Déployé).

Étape 17 Vérifiez la mise à niveau.

a) Ouvrez l'interface utilisateur Cisco Secure Workload dans votre navigateur.
b) Dans le volet de navigation de gauche, cliquez sur **Platform (plateforme) > Upgrade/Reboot/Shutdown (Mise à niveau/redémarrage/arrêt).**
c) Cliquez sur **History** (Historique).
d) Vérifiez que l'état dans la colonne **Status** (État) est **Succeeded** (Réussite).

Prochaine étape

Après la mise à niveau, apportez les modifications nécessaires pour bénéficier des améliorations de cette version :

- Si vous avez activé IPv6, vous pouvez accéder à l'interface Web de Cisco Secure Workload en utilisant une adresse IPv4 ou IPv6. Par défaut, les agents continuent de se connecter à la grappe à l'aide d'IPv4. Si vous souhaitez que les agents logiciels puissent communiquer avec la grappe à l'aide d'IPv6 :

  1. Dans le volet de navigation, choisissez **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)**.
  2. Configurez le paramètre **Sensor VIP FQDN** (Nom de domaine complet VIP du capteur) comme décrit dans le Guide de l'utilisateur disponible sur le portail Web Cisco Secure Workload.

- Pour la mise en grappe améliorée des charges de travail standard de Kubernetes dans les portées, reportez vous à Mises à niveau vers les versions 3.9, 3.8 et 3.7 : activation de la mise en grappe améliorée des charges de travail Kubernetes dans la découverte de politiques, à la page 32.

Mise à niveau vers la version Cisco Secure Workload 3.7.x

Mise à niveau vers la version Cisco Secure Workload 3.7.1.59

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.7.1.5, 3.7.1.22, 3.7.1.39 ou 3.7.1.51.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.59.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.7.1.59-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau **« Service à la clientèle »** dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.7.1.51

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.7.1.5, 3.7.1.22 ou 3.7.1.39.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.51.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.7.1.51-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau **« Service à la clientèle »** dispose d'une clé SSH chargée à des fins de dépannage.

- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.

b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.7.1.39

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.7.1.5 ou 3.7.1.22.

Avant de commencer

⚠

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.39.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.7.1.39-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.
a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.
b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

   Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version 3.7.1.22 de Cisco Secure Workload

Vous pouvez effectuer une mise à niveau vers cette version à partir de la version 3.7.1.5.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.22.

Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.7.1.22-1.noarch.rpm`

- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version 3.7.1.5 de Cisco Secure Workload

Vous pouvez effectuer une mise à niveau vers cette version à partir de n'importe quelle version 3.6, mais il est recommandé d'effectuer la mise à niveau vers la dernière version de correctif 3.6.1.x avant de procéder à la mise à niveau vers cette version.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

Gardez ces points à l'esprit :

- Orchestrateurs externes de Kubernetes AKS : après la mise à niveau, les orchestrateurs externes AKS seront en lecture seule; si vous souhaitez apporter des modifications après la mise à niveau, créez un nouveau connecteur Azure et activez l'option **Managed Kubernetes services** (Services gérés Kubernetes).
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour cette mise à niveau.
- Si des connecteurs ISE sont configurés, vérifiez que leurs certificats TLS comportent des sections Subject Alternative Name (SAN). Après la mise à niveau, le connecteur ISE ne se connectera pas aux terminaux ISE qui présentent d'anciens certificats TLS CN uniquement. Ne procédez pas à la mise à niveau avant que les certificats ISE TLS ne soient régénérés avec les extensions SAN.
- **Licence**
  - Si votre déploiement Cisco Secure Workload ne dispose pas actuellement de licences valides (ou est en dehors de la période d'évaluation), vous devez enregistrer des licences valides avant de procéder à la mise à niveau.
  - Des privilèges d'administrateur de site sont nécessaires pour gérer les licences.

- Pour afficher l'état de vos licences : Sur le portail Web Cisco Secure Workload, sélectionnez **Monitoring** > **Licenses (surveillance des licences)** . Si l'enregistrement de votre licence de cluster n'est pas conforme, vous verrez une bannière avec un lien **Take Action** (Prendre des mesures). Pour savoir comment obtenir et enregistrer des licences, dans le portail Web Secure Workload, sélectionnez **Help (Help)** > **Page-level Help (Aide au niveau de la page)** et recherchez Licenses.

Procédure

Étape 1 Téléchargez les fichiers RPM applicables à votre déploiement à partir de Cisco.com :

a) Accédez à https://software.cisco.com/download/home/286309796/type.

b) Téléchargez le cas échéant :

- Pour un système 8-RU ou 39-RU, téléchargez les RPM suivants :
  - tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- Pour un système virtuel, téléchargez les RPM suivants :
  - tetration_os_ova_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-5.el6.x86_64.rpm

c) Vérifiez que la somme de contrôle MD5 des RPM téléchargés correspond à la somme de contrôle MD5 dans CCO.

Étape 2 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web Cisco Secure Workload, cliquez sur **Settings** (Paramètres) et sélectionnez **Maintenance** (Entretien).

b) Dans le volet gauche, sélectionnez **Service Status** (État du service).

c) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

d) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 3 Dans le menu de navigation de gauche, sélectionnez **Maintenance** > **Upgrade** (Entretien > Mise à niveau).

Étape 4 Si nécessaire, cliquez sur l'onglet **Upgrade** (Mise à niveau).

Étape 5 Suivez les instructions à l'écran. Veillez à ne sauter aucune étape.

Utilisez l'option **Upgrade** (Mise à niveau), ET NON l'option de mise à niveau du correctif.

Étape 6 Cliquez sur **Envoyer le lien de mise à niveau**.

Un utilisateur connecté avec un rôle d'administrateur de site ou de service d'assistance à la clientèle recevra un courriel avec un lien hypertexte qui devra être utilisé pour effectuer la mise à niveau. L'objet du courriel sera :

```
[Tetration Analytics] Upgrade Initiation Link
```

Ouvrez le courriel et copiez l'URL **Upgrade Cluster** (Mise à niveau de la grappe).

Sinon, vous pouvez récupérer l'URL de mise à niveau à partir de la page **Maintenance** > **Explore** (Entretien > Exploration) en saisissant les informations suivantes :

- Action sur l'instantané :**POST**
- Hôte de l'instantané :**orchestrator.service.consul**
- Chemin de l'instantané :**upgrade_url**

Étape 7 Dans Google Chrome, collez l'URL de mise à niveau dans le champ d'adresse et appuyez sur **Entrée**.

Le portail de configuration de Cisco Secure Workload s'affiche. Notez que Google Chrome est le seul navigateur Web pris en charge pour la mise à niveau.

Étape 8 Dans le portail de configuration de Cisco Secure Workload, vous devez charger les fichiers RPM dans un ordre spécifique selon votre configuration. Pour charger les fichiers RPM, procédez comme suit :

a) Cliquez sur **Choose file** (Choisir le fichier).
b) Naviguez jusqu'à un fichier RPM, sélectionnez-le, puis cliquez sur **Open** (Ouvrir).
c) Cliquez sur **Upload** (Téléverser).
d) Répétez les étapes **a** à **c** pour chaque fichier RPM.
La liste des fichiers RPM sur la page ne se met pas à jour au fur et à mesure que vous les téléchargez, ce qui est normal. Si vous constatez une erreur après le chargement du fichier *tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm*, attendez 5 à 10 minutes, puis rechargez la page. Vous devriez maintenant pouvoir afficher la liste des RPM téléchargés.

Pour un système 8-RU ou 39-RU, chargez les fichiers suivants dans l'ordre indiqué :

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm

Pour un système virtuel, chargez les fichiers suivants dans l'ordre indiqué :

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.7.1.5-1.noarch.rpm

Étape 9 Cliquez sur **Continue** (Continuer).
Le portail **Site Config** 'Configuration du site) s'affiche.

Étape 10 (Facultatif) Sous **General** (Général), modifiez la clé publique SSH et cliquez sur **Next** (Suivant).

Étape 11 (Facultatif) Sous **Email** (Adresse de courriel), modifiez l'administrateur de l'interface utilisateur ou l'adresse de courriel de l'administrateur, puis cliquez sur **Next** (Suivant).

Étape 12 (Facultatif) Sous **L3**, autorisez la grappe à utiliser des adresses IPv6 en plus des adresse IPv4 pour certaines connectivités de la grappe après la mise à niveau. Pour activer IPv6 :

a) Cochez la case **IPv6**.
b) Saisissez les adresses IPv6 en notation CIDR pour les commutateurs à ressort à lame 1 et 2.
c) Saisissez la passerelle par défaut IPv6 du commutateur à ressort à lame1 et ressort à lame2.
d) Cliquez sur **Next** (suivant).

Si vous activez IPv6 sur cette page, vous devez également configurer les champs IPv6 sur la page **Network** (Réseau), décrite à l'étape suivante.

Important Pour les exigences et les limites du mode pile double, consultez Exigences et limites du mode double pile (prise en charge d'IPv6), à la page 2.

Étape 13 Sous **Network** (Réseau) :

a) Au besoin, modifiez les valeurs de **CIMC Internal Network (Réseau interne CIMC)**, de **CIMC Internal Network Gateway (Passerelle réseau interne CIMC)**, de **DNS Resolve (Résolveur DNS)** et de **DNS Domain (Domaine DNS).**
b) **Important!** Ne modifiez, ni ne supprimez la valeur **External Network** (Réseau externe) existante. Cependant, vous pouvez ajouter des réseaux IPv4 supplémentaires.
c) Si vous avez activé IPv6 à la page L3, la case **IPv6** est automatiquement cochée. Préciser les adresses IPv6 réservées pour une utilisation de Cisco Secure Workload par :

1. Saisissez le réseau externe IPv6 en notation CIDR.
2. (Facultatif) Pour utiliser l'adresse IPv6 uniquement pour des adresses spécifiées, saisissez les adresses IP IPv6 externes individuelles.

Remarque:

- Les trois premières adresses IPv6 dans le champ Réseau externe IPv6 sont toujours réservées pour les commutateurs de la grappe Cisco Secure Workload et ne doivent pas être utilisées à d'autres fins.
- Pour une grappe 39 RU, vérifiez qu'au moins 29 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.
- Pour une grappe 8 RU, vérifiez qu'au moins 20 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.

d) Cliquez sur **Next** (suivant).

Étape 14 (Facultatif) Sous **Service** (Service), modifiez les valeurs NTP et SMTP, puis cliquez sur **Next** (Suivant).

Si vous devez modifier les valeurs syslog (le cas échéant), utilisez l'appareil NAT.

Étape 15 Sous **Security**(sécurité), activez ou désactivez les chiffrements SSL renforcés pour les connexions des agents, puis cliquez sur **Next**(suivant).

Vous ne pouvez pas modifier les valeurs sous les onglets **UI** (Interface utilisateur), **Advanced** (Avancé) et **Recovery** (Récupération).

Sous **Recovery** (Récupération), si la grappe est configurée pour être une grappe de secours, elle sera déployée en mode veille, ce qui inclut des fonctionnalités réduites (uniquement pour prendre en charge le mode veille à chaud).

Étape 16 Cliquez sur **Continue** (Continuer).
Les vérifications suivantes sont effectuées au cours du processus de mise à niveau pour s'assurer que :

- Les versions RPM sont correctes
- La grappe est intègre
- Les renseignements sur le site que vous avez fournis sont valides
- Les commutateurs sont configurés correctement et peuvent être mis à niveau vers une version plus récente du logiciel NX-OS
- Les champs de renseignements sont validés
- Le protocole NTP est synchronisé avant le début du déploiement
- Le nœud de nom et de nom secondaire ne sont pas dans un état de basculement

Les vérifications peuvent prendre de quelques minutes à une heure si les commutateurs de la grappe doivent être mis à niveau. Une fois les vérifications terminées, vous recevrez un courriel avec pour objet : `TETRATION CLUSTER MyCluster: Verify Token` (GRAPPE TETRATION MaGrappe : Jeton de vérification). Le message contient un jeton dont vous aurez besoin pour continuer la mise à niveau. Copiez le jeton de ce courriel.

Étape 17 Dans le portail de configuration de Cisco Secure Workload, collez le jeton dans le champ **Validation Token** (jeton de validation) et cliquez sur **Continue**(continuer) .

Important Ne cochez pas la case **Ignore instance stop failures** (Ignorer les échecs d'arrêt de l'instance), à moins qu'un collaborateur de Cisco ne vous le demande expressément.

Le processus de mise à niveau est lancé. Dans la version 3.7.1.5, les machines virtuelles de l'orchestrateur seront mises à niveau avant les autres composants. Cela peut prendre de 30 à 60 minutes, pendant lesquels la barre de progression passera de 0 à 100 %. Une fois les mises à niveau des orchestrateurs terminées, les autres composants seront mis à niveau et la barre de progression recommencera à 0 %. Lorsque la barre de progression verte atteint 100 %, la mise à niveau est terminée. Toutes les instances affichent l'état « Deployed » (Déployé).

Étape 18 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 19 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Prochaine étape

Après la mise à niveau, apportez les modifications nécessaires pour bénéficier des améliorations de cette version :

- Consultez Prochaine étape, à la page 46.
- Pour la mise en grappe améliorée des charges de travail standard de Kubernetes dans les portées, reportez vous à Mises à niveau vers les versions 3.9, 3.8 et 3.7 : activation de la mise en grappe améliorée des charges de travail Kubernetes dans la découverte de politiques, à la page 32.

Mises à niveau vers les versions 3.9, 3.8 et 3.7 : activation de la mise en grappe améliorée des charges de travail Kubernetes dans la découverte de politiques

Cette fonctionnalité s'applique uniquement à Kubernetes standard (dans la configuration de l'orchestrateur, le « Type de gestionnaire K8s » est « Aucun »).

Si vous avez déjà configuré des orchestrateurs externes Kubernetes, vous pouvez activer une amélioration des versions 3.9, 3.8 et 3.7 qui améliore la précision des résultats de la mise en grappe ADM pour les charges de travail Kubernetes, en utilisant les métadonnées d'étiquettes Kubernetes pour la mise en grappe.

Pour activer cette amélioration, effectuez les deux opérations suivantes pour chaque orchestrateur Kubernetes standard après la mise à niveau :

- Dans la configuration de l'orchestrateur externe Kubernetes standard (sous **Manage (Gestion) > External Orchestrators (Orchestrateurs externes)**), activez **Use for policy discovery clustering (utiliser pour la mise en grappe de découverte de politiques**) et enregistrez les modifications.
- Ajoutez les privilèges suivants au ClusterRole lié au compte de service.

Ressources	Verbes Kubernetes
contrôleurs de duplication	[obtenir la liste de surveillance]
replicasets	[obtenir la liste de surveillance]
deployments	[obtenir la liste de surveillance]
daemonsets	[obtenir la liste de surveillance]
statefulsets	[obtenir la liste de surveillance]
d'emplois	[obtenir la liste de surveillance]
cronjobs	[obtenir la liste de surveillance]

Un exemple de fichier clusterrole.yaml qui inclut ces privilèges (votre version peut être légèrement différente) :

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
```

```
  name: tetration.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
```

Mise à niveau vers la version Cisco Secure Workload 3.6.x

Mise à niveau vers la version Cisco Secure Workload 3.6.1.47

Vous pouvez effectuer une mise à niveau vers cette version à partir de toute version antérieure 3.6.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.47.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.6.1.47-1.noarch.rpm`

- Vous devez sauvegarder votre système avant d'effectuer une mise à niveau. Pour en savoir plus, consultez les renseignements sur la sauvegarde et la restauration des données (DBR) dans le guide de l'utilisateur, y compris la sous-section sur les mises à niveau.
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.6.1.36

Vous pouvez effectuer une mise à niveau vers cette version à partir de toute version antérieure 3.6.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.36.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.6.1.36-1.noarch.rpm`

- Vous devez sauvegarder votre système avant d'effectuer une mise à niveau. Pour en savoir plus, consultez les renseignements sur la sauvegarde et la restauration des données (DBR) dans le guide de l'utilisateur, y compris la sous-section sur les mises à niveau.
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.

b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).

c) Cliquez sur **History** (Historique).

d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.6.1.21

Vous pouvez effectuer une mise à niveau vers cette version à partir de toute version antérieure 3.6.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.21.

  Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.6.1.21-1.noarch.rpm`

- Vous devez sauvegarder votre système avant d'effectuer une mise à niveau. Pour en savoir plus, consultez les renseignements sur la sauvegarde et la restauration des données (DBR) dans le guide de l'utilisateur, y compris la sous-section sur les mises à niveau.
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version 3.6.1.17 de Cisco Secure Workload

Vous pouvez effectuer une mise à niveau vers la version 3.6.1.17 à partir de la version 3.6.1.5.

Avant de commencer

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre les problèmes avant de continuer.

- Téléchargez le paquet d'installation :

  Dans votre navigateur, accédez à https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.17.

Téléchargez le fichier RPM suivant : `tetration_os_patch_k9-3.6.1.17-1.noarch.rpm`

- Vous devez sauvegarder votre système avant d'effectuer une mise à niveau. Pour en savoir plus, consultez les renseignements sur la sauvegarde et la restauration des données (DBR) dans le guide de l'utilisateur, y compris la sous-section sur les mises à niveau.
- Assurez-vous qu'un compte de niveau « Service à la clientèle » dispose d'une clé SSH chargée à des fins de dépannage.
- Vous devez effectuer la procédure suivante en tant qu'utilisateur avec des privilèges d'administrateur de site ou de service d'assistance à la clientèle.
- Google Chrome est le seul navigateur pris en charge pour une partie de cette mise à niveau.

Procédure

Étape 1 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface Web de Cisco Secure Workload, choisissez **Dépannage : État du service** dans le menu de navigation sur le côté gauche de la fenêtre.

b) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

c) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 2 Dans l'interface Web de Cisco Secure Workload, dans le menu situé à gauche de la fenêtre, cliquez sur **Platform** (Plateforme) > **Upgrade/Reboot/Shutdown** (Mettre à niveau/Redémarrer/Arrêt).

Étape 3 Suivez les instructions qui s'affichent.

Résolvez les problèmes détectés par la vérification préalable avant de continuer.

Assurez-vous que la **mise à niveau des correctifs** est sélectionnée. (Il s'agit d'un correctif de mise à niveau).

Cliquez sur **Envoyer le lien de mise à niveau**.

Étape 4 Recherchez un courriel dont l'objet est le suivant :

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

Ce message comprend un lien hypertexte que vous devez utiliser pour effectuer la mise à niveau.

Étape 5 Dans le courriel, cliquez sur le bouton **Patch Upgrade <Cluster>** (Mise à niveau du correctif <Grappe>) pour ouvrir l'interface utilisateur de configuration deCisco Secure Workload. Vous devez utiliser le navigateur Google Chrome.

Étape 6 Cliquez sur **Choose file** (Choisir le fichier).

Étape 7 Accédez au correctif RPM que vous avez téléchargé ci-dessus, sélectionnez-le et cliquez sur **Open** (Ouvrir).

Étape 8 Cliquez sur **Upload** (Téléverser).

Le téléchargement du RPM lancera la mise à niveau.

Au cours de ce processus, vous perdrez temporairement la connectivité à l'interface utilisateur de configuration.

Étape 9 Attendez quelques minutes pour retrouver l'accès à l'interface Web et afficher les résultats de la mise à niveau.

Si la mise à niveau pose problème, une bannière rouge s'affiche. Cliquez sur l'image en forme de livre pour afficher les journaux.

Étape 10 Vérifiez la mise à niveau.

a) Ouvrez l'interface Web de Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que la colonne État indique **Succeeded** (Réussite).

Étape 11 Si la mise à niveau a réussi, cliquez sur **Disable Patch Upgrade Link** (Désactiver le lien de mise à jour des correctifs).

Mise à niveau vers la version Cisco Secure Workload 3.6.1.5

Vous pouvez effectuer une mise à niveau vers cette version à partir de n'importe quelle version 3.5.1.x, mais il est recommandé d'effectuer la mise à niveau vers la dernière version du correctif 3.5.1.x avant de procéder à la mise à niveau vers cette version.

Ces instructions sont valides pour les déploiements matériels et virtuels.

Avant de commencer

⚠

Mise en garde Ne pas mettre à niveau si des nœuds sont actuellement à l'état hors service ou si des services ne sont pas intègres. Avant de continuer, communiquez avec le Centre d'assistance technique de Cisco (TAC) pour résoudre tout problème.

Conditions préalables supplémentaires :

- **Licence**

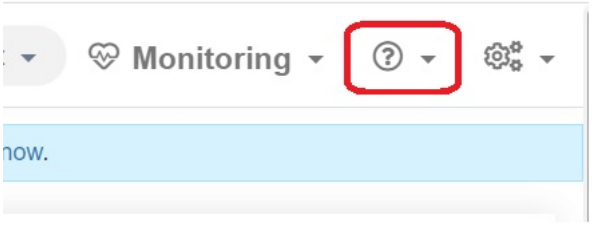
  Si votre déploiement Tetration ne dispose pas actuellement de licences valides (ou est en dehors de la période d'évaluation), vous devez enregistrer des licences valides avant de procéder à la mise à niveau.

  Des privilèges d'administrateur de site sont nécessaires pour gérer les licences.

  Pour voir l'état de vos licences :

  Dans le portail Web Tetration , choisissez **Monitoring > Licenses (Superviser > Licences)** Si l'enregistrement de votre licence de cluster n'est pas conforme, vous verrez une bannière avec un lien **Take Action** (Prendre des mesures).

  Pour en savoir plus sur l'obtention et l'enregistrement de licences, consultez le Guide de l'utilisateur sur le portail Web de Tetration en cliquant ici :



Recherchez « Licences » dans le guide de l'utilisateur.

- **Prise en charge d'IPv6 (mode double pile)**

  (Facultatif) Les grappes Cisco Secure Workload fonctionnant sur du matériel physique peuvent être configurées de manière à utiliser IPv6 en plus d'IPv4 pour certaines communications avec la grappe et au sein de cette dernière. (Cisco Secure Workload gère déjà le trafic IPv6 à des fins de politique).

  Vous ne pouvez activer cette fonctionnalité que lors du déploiement initial ou de la mise à niveau vers la version 3.6.1.5.

  Si vous envisagez d'activer la connectivité à double pile (IPv6), consultez Exigences et limites du mode double pile (prise en charge d'IPv6), à la page 2.

- **Autres fonctionnalités**

  Incidences propres aux fonctionnalités qui peuvent nécessiter des mesures avant la mise à niveau :

  - **Intégration Cisco Firepower Management Center (FMC) :**

    Si vous mettez à niveau Cisco Secure Workload et que vous souhaitez continuer à utiliser cette intégration, vous devez d'abord mettre à niveau FMC vers la version requise.

    Cette intégration dans la version 3.6 est très différente de l'implémentation dans la version 3.5. Lisez attentivement la description et les exigences dans la version 3.6 du *Guide d'intégration de Cisco Secure Workload et de Cisco Firepower Management Center*, disponible à partir de https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html.

    Après la mise à niveau de Cisco Secure Workload, les politiques de préfiltre de FMC seront converties en politiques de contrôle d'accès et les filtres d'inventaire seront convertis en objets dynamiques.

  - **Connecteurs AWS :**

    Les connecteurs AWS existants seront supprimés lors de la mise à niveau. Vous devez recréer les nouveaux connecteurs infonuagiques AWS après la mise à niveau. Si nécessaire, veuillez noter les informations configurées avant la mise à niveau.

  - Orchestrateurs externes de Kubernetes EKS

    Après la mise à niveau, les orchestrateurs externes EKS seront en lecture seule; si vous souhaitez apporter des modifications après la mise à niveau, créez un nouveau connecteur AWS et activez l'option **Managed Kubernetes services** (Services gérés Kubernetes).

  - **Connecteur d'exportation de données :**

    La prise en charge du connecteur d'exportation de données (fonctionnalité alpha) a été supprimée de cette version. Si vous avez configuré le connecteur d'exportation de données; il est recommandé de le désactiver ou de le supprimer avant de procéder à la mise à niveau vers cette version.

  - **Autres modifications :**

D'autres changements de comportement qui ne nécessitent pas d'action avant la mise à niveau sont décrits dans les notes de version dans la version 3.6.1.5, disponibles à l'adresse suivante https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html.

- Cette mise à niveau ne nécessite PAS de nouvelle adresse IP publique routable.
- Des privilèges de service d'assistance à la clientèle sont nécessaires pour effectuer cette mise à niveau.
- Assurez-vous qu'un compte d'utilisateur avec des privilèges de service d'assistance à la clientèle dispose d'une clé SSH chargée à des fins de dépannage. Pour en savoir plus, consultez « Importer une clé publique SSH » dans le guide de l'utilisateur disponible sur le portail Web Tetration.
- Vous devez sauvegarder votre système avant d'effectuer une mise à niveau. Pour en savoir plus, consultez les renseignements sur la sauvegarde et la restauration des données (DBR) dans le guide de l'utilisateur, y compris la sous-section sur les mises à niveau.
- Google Chrome est le seul navigateur pris en charge par le portail d'installation de Cisco Secure Workload, un portail dédié requis pour une partie de cette mise à niveau.

Procédure

Étape 1 Téléchargez les fichiers RPM applicables à votre déploiement à partir de Cisco.com :

a) Accédez à https://software.cisco.com/download/home/286309796/type.

b) Téléchargez le cas échéant :

- Pour un système 8-RU ou 39-RU, téléchargez les RPM suivants :
  - `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
  - `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`
  - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
  - `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
- Pour un système virtuel, téléchargez les RPM suivants :
  - `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`
  - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
  - `tetration_os_enforcement_k9-3.6.1.5-5.el6.x86_64.rpm`

c) Vérifiez que le MD5 de chaque téléchargement de RPM correspond au MD5 dans CCO.

Étape 2 Vérifiez l'intégrité du système. Vous ne pouvez pas effectuer la mise à niveau si des services ne sont pas intègres.

a) Dans l'interface graphique utilisateur de Cisco Tetration, cliquez sur le bouton Paramètres et choisissez **Maintenance** (Entretien).
b) Dans le volet gauche, cliquez sur **Service Status** (État du service).
c) Recherchez les cercles rouges du graphique qui indiquent des services non intègres.

   Sinon, pour afficher un tableau de l'intégrité du service, cliquez sur le bouton de liste en haut du graphique, cliquez sur **Expand All** (Développer tout) et faites défiler la page vers le bas pour afficher l'état de tous les services.

d) Si des services ne sont pas intègres, effectuez les correctifs nécessaires pour les rendre intègres avant de procéder à la mise à niveau.

Étape 3 Dans le menu de navigation de gauche, cliquez sur **Maintenance > Upgrade** (Entretien > Mise à niveau).

Étape 4 Si nécessaire, cliquez sur l'onglet **Upgrade** (Mise à niveau).

Étape 5 Suivez les étapes à l'écran. Ne sautez aucune étape.

Utilisez l'option **Upgrade** (Mise à niveau), PAS l'option de mise à niveau du correctif.

Étape 6 Après avoir cliqué sur **Send Upgrade Link** (Envoyer un lien de mise à niveau), recherchez le message courriel qui en résulte.

Un utilisateur qui s'est connecté avec un rôle d'administrateur de site ou de service d'assistance à la clientèle recevra un courriel avec un lien hypertexte qui devra être utilisé pour effectuer la mise à niveau. L'objet du courriel sera :

`[Tetration Analytics] Upgrade Initiation Link` ([Tetration Analytics] Lien de lancement de la mise à niveau)

Ouvrez le message électronique et copiez l'URL **Upgrade Cluster** (Mettre à niveau la grappe).

Sinon, vous pouvez récupérer l'URL de mise à niveau à partir de la page **Maintenance > Explore (Entretien > Explorer)** en saisissant les renseignements suivants :

- Action sur l'instantané :**POST**
- Hôte de l'instantané :**orchestrator.service.consul**
- Chemin de l'instantané :**upgrade_url**

Étape 7 Ouvrez un nouvel onglet du navigateur Google Chrome, collez l'URL de mise à niveau dans le champ d'adresse, puis appuyez sur la touche **Entrée**.

Cela ouvre le portail de configuration de Cisco Secure Workload, qui n'est pris en charge que par le navigateur Google Chrome.

Étape 8 Dans le portail de configuration de Cisco Secure Workload, vous devez charger les fichiers RPM dans un ordre spécifique, selon votre configuration.

Pour un système 8-RU ou 39-RU, chargez les fichiers suivants dans l'ordre indiqué :

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`
3. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`

6. `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`

Pour un système virtuel, chargez les fichiers suivants dans l'ordre indiqué :

1. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
2. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
3. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
4. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`
5. `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`

Pour charger chaque RPM, procédez comme suit :

a) Cliquez sur **Choose file** (Choisir le fichier).
b) Accédez à un RPM, sélectionnez-le et cliquez sur **Open** (Ouvrir).
c) Cliquez sur **Upload** (Téléverser).

La liste des RPM sur la page ne se met pas à jour lorsque vous chargez chaque RPM. C'est normal.

Si vous constatez une erreur après le chargement du fichier `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`, attendez simplement environ 5 à 10 minutes, puis rechargez la page. Vous devriez voir la liste des RPM téléchargés s'afficher après le rechargement de la page.

d) Répétez ces sous-étapes pour chaque RPM.

Étape 9 Cliquez sur **Continue** (Continuer).

Le portail **Site Config** (Configuration du site) s'ouvre.

Étape 10 Sous l'onglet **General** (General) :

(Facultatif) Modifiez la clé publique SSH.

Étape 11 Cliquez sur **Next** (suivant).

Étape 12 Sous l'onglet **Email** (Courriel) :

(Facultatif) Modifiez l'adresse courriel de l'administrateur de l'interface utilisateur ou l'adresse courriel d'alerte Admiral.

Étape 13 Cliquez sur **Next** (suivant).

Étape 14 Sur l'onglet **L3** :

(Facultatif) Permet à la grappe d'utiliser IPv6 en plus d'IPv4 pour certaines connectivités de grappe après la mise à niveau.

Important! Pour connaître les exigences et les limites, consultez le lien dans les conditions préalables à cette procédure.

Pour activer IPv6 :

a) Cochez la case **IPv6**.
b) Saisissez **l'adresse IPv6 en notation CIDR** pour les commutateurs à ressort à lame 1 et 2.
c) Saisissez la **passerelle par défaut IPv6** du commutateur à ressort à lame1 et ressort à lame2.

Si vous activez IPv6 sur cette page, vous devez également configurer les champs IPv6 de la page **Network**(Réseau), ci-dessous.

Étape 15 Cliquez sur **Next** (suivant).

Étape 16 Sous l'onglet **Network** (Réseau) :

- Au besoin, modifiez les valeurs de **CIMC Internal Network (Réseau interne CIMC)**, de **CIMC Internal Network Gateway (Passerelle réseau interne CIMC)**, de **DNS Resolve (Résolveur DNS)** et de **DNS Domain (Domaine DNS).**
- **Important!** Ne modifiez, ni ne supprimez la valeur **External Network** (Réseau externe) existante. Cependant, vous pouvez ajouter des réseaux IPv4 supplémentaires.
- Si vous avez activé IPv6 sur la page L3 :

  La case **IPv6** est automatiquement cochée.

  Préciser les adresses IPv6 réservées à l'utilisation de Cisco Secure Workload :

  a. Saisissez le paramètre **IPv6 External Network in CIDR notation** (réseau externe IPv6 en notation CIDR).

  b. (Facultatif) Pour utiliser IPv6 uniquement pour des adresses spécifiées, entrez les différentes **adresses IP IPv6 externes**.

  À retenir :

  - Les trois premières adresses IPv6 dans le champ Réseau externe IPv6 sont toujours réservées pour les commutateurs de la grappe Cisco Secure Workload et ne doivent pas être utilisées à d'autres fins.
  - Pour une grappe 39 RU, vérifiez qu'au moins 29 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.
  - Pour une grappe 8 RU, vérifiez qu'au moins 20 adresses IPv6 sont disponibles dans la liste du réseau externe IPv6 ou dans la liste d'adresses IP IPv6 externes.

Étape 17 Cliquez sur **Next** (suivant).

Étape 18 Dans l'onglet **Service** (Service) :

(Facultatif) Modifiez les valeurs NTP et SMTP.

Si vous devez modifier les valeurs syslog (le cas échéant), utilisez l'appareil NAT.

Étape 19 Cliquez sur **Next** (suivant).

Étape 20 Sous l'onglet **Security** (Sécurité) :

Cochez ou décochez **Strong SSL Ciphers for Agent Connections** (chiffrements SSL renforcés pour les connexions d'agents).

Étape 21 Cliquez sur **Next** (suivant).

Vous ne pouvez modifier aucune valeur sous l'onglet **UI** (interface utilisateur).

Étape 22 Cliquez sur **Next** (suivant).

Vous ne pouvez modifier aucune valeur de l'onglet **Advanced** (Avancé).

Étape 23 Cliquez sur **Next** (suivant).

Étape 24 Dans l'onglet **Recovery** (Récupération) :

Si la grappe est configurée pour être une grappe de secours, elle sera déployée en mode veille, ce qui inclut des fonctionnalités réduites (uniquement pour prendre en charge le mode veille à chaud).

Vous ne pouvez modifier aucune valeur de cet onglet.

Étape 25 Cliquez sur **Continue** (Continuer).

Le processus de mise à niveau commence.

Le processus de mise à niveau vérifie que :

- Les versions RPM sont correctes
- La grappe est intègre
- Les renseignements sur le site que vous avez fournis sont valides
- Les commutateurs sont configurés correctement
- Les champs de renseignements sont validés
- Le protocole NTP est synchronisé avant le début du déploiement
- Le nœud de nom et de nom secondaire ne sont pas dans un état de basculement

Cette vérification prendra plusieurs minutes. Une fois les vérifications terminées, vous recevrez un courriel avec un objet semblable à celui-ci :

`TETRATION CLUSTER MyCluster: Verify Token` (GRAPPE TETRATION MaGrappe : Jeton de vérification)

Le message contient un jeton dont vous aurez besoin pour continuer la mise à niveau.

Étape 26 Copiez le jeton du corps du message électronique.

Étape 27 Dans le portail d'installation de Cisco Secure Workload, collez le jeton dans le champ **Validation Token** (jeton de validation).

Important! Ne cochez pas la case **Ignore instance stop failures** (Ignorer les échecs d'arrêt de l'instance), à moins qu'un collaborateur de Cisco ne vous le demande expressément.

Étape 28 Cliquez sur **Continue** (Continuer).

L'installation de la mise à niveau commence. Lorsque la barre de progression verte atteint 100 %, la mise à niveau est terminée. Toutes les instances afficheront l'état « Deployed » (déployé).

Étape 29 Vérifiez la mise à niveau.

a) Ouvrez le portail Web Cisco Secure Workload dans votre navigateur.
b) Dans le menu de navigation noir sur la gauche, choisissez **Platform > Upgrade/Reboot/Shutdown** (Plateforme > Mise à niveau/redémarrage/arrêt).
c) Cliquez sur **History** (Historique).
d) Vérifiez que l'état de la mise à niveau indique **Succeeded** (Réussie).

Prochaine étape

Si vous avez activé IPv6 :

- Vous pouvez accéder à l'interface Web de Cisco Secure Workload en utilisant IPv6 ou IPv4.
- Par défaut, les agents logiciels continuent de se connecter à la grappe à l'aide d'IPv4. Si vous souhaitez que les agents logiciels puissent communiquer avec la grappe à l'aide d'IPv6, effectuez les actions suivantes :

  1. Sur l'interface utilisateur de Cisco Secure Workload, dans le volet de navigation de gauche, cliquez sur **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)** .
  2. Configurez le paramètre **Sensor VIP FQDN** (Nom de domaine complet VIP du capteur). Pour en savoir plus, consultez l'aide présente sur la page ou le guide de l'utilisateur de Cisco Secure Workload disponible sur Cisco.com.

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.