



# Déployer des agents logiciels sur les charges de travail

---

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

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

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

- [Déployer des agents logiciels, on page 2](#)
- [Exclusions de sécurité, on page 32](#)
- [Gestion des services des agents, on page 35](#)
- [Application des politiques par le biais d'agents, on page 37](#)
- [Configuration de l'agent logiciel, à la page 62](#)
- [Afficher l'état détaillé de l'agent dans le profil de charge de travail, on page 75](#)
- [Relocalisation des agents, on page 76](#)
- [Générer un jeton d'agent, on page 80](#)
- [Changement de l'adresse IP de l'hôte lorsque la mise en application est activée, on page 81](#)
- [Mise à niveau des agents logiciels, à la page 82](#)
- [Suppression des agents logiciels, à la page 86](#)
- [Données collectées et exportées par les agents de charge de travail, on page 90](#)
- [Alertes de mise en application, on page 92](#)
- [Alertes de capteurs, on page 99](#)

# Déployer des agents logiciels



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

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

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

## Supported Platforms and Requirements

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

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

## Installation des agents Linux pour une visibilité approfondie et une application

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

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

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

## Méthodes prises en charge pour l'installation des agents Linux

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

- [Installer l'agent Linux à l'aide de la méthode du programme d'installation du script de l'agent, on page 4](#)
  - [Prise en charge des agents pour la plateforme de mise en réseau Blufield de NVIDIA](#)
- [Installer l'agent Linux à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 3](#)

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

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

#### Prérequis

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

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

#### Procédure

##### Étape 1

Accédez à Méthodes d'installation des agents :

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

##### Étape 2

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

##### Étape 3

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

##### Étape 4

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

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

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

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

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

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

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



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

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

### Procédure

**Étape 1** Accédez à Méthodes d'installation des agents :

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

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

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

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

**Étape 4** Choisissez le détenteur pour installer les agents.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

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

```

**Note**

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

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

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

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

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

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

### Exigences et prérequis

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

### Installation des agents

L'installation suit un processus de type Linux.

#### 1. Accédez à Méthodes d'installation des agents :

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

#### 2. Dans l'onglet **Installer** (Programme d'installation), sélectionnez **Agent Script Installer** (Programme d'installation de script d'agent).

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

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



---

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

---

#### 4. Choisissez le détenteur pour installer les agents.



---

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

---

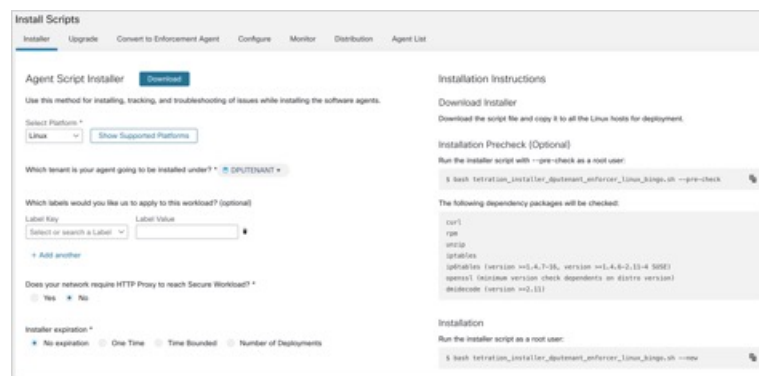
#### 5. Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.

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

#### 7. Dans la section **Installer expiration** (expiration du programme d'installation), sélectionnez-en une option parmi celles disponibles :

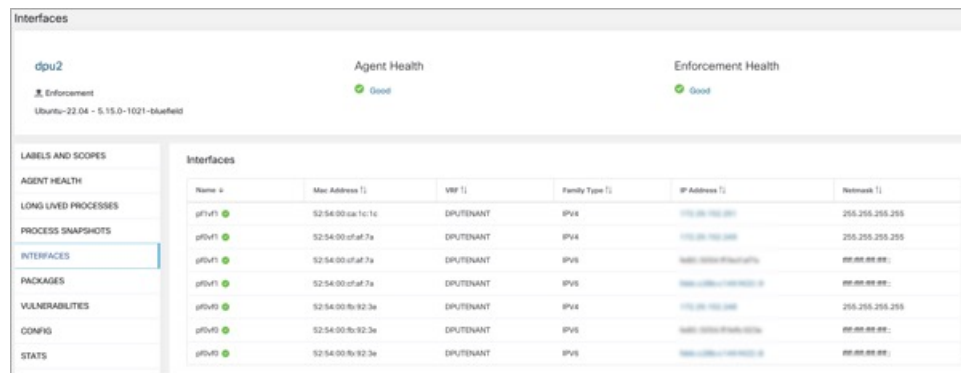
- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
  - Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
  - Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
  - Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.
8. Cliquez sur **Download** (Télécharger) pour télécharger le script d'installation de Linux sur la DPU à l'aide de l'un de ses périphériques réseau.
  9. Exécutez le script d'installation. Pour en savoir plus, consultez [Installer l'agent Linux à l'aide de la méthode du programme d'installation du script de l'agent](#).

Figure 1: Script d'installation



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

Figure 2: Mappage d'interface



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



## Vérifier l'installation de l'agent Linux

### Procédure

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

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

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

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

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

## Installation des agents Windows pour une visibilité approfondie et pour application

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

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

### Méthodes prises en charge pour l'installation des agents Windows

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

- [Installer l'agent Windows à l'aide de la méthode du programme d'installation du script de l'agent, on page 10](#)
- [Installer l'agent Windows à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 12](#)

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

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

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



- Note**
- L'agent Windows installé prend en charge la visibilité approfondie et la mise en application.
  - Le paramètre par défaut est Disabled (désactivé). Pour activer l'application, consultez [Creating an Agent Config Profile, on page 65](#).

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

### Procédure

- Étape 1** Accédez à Méthodes d'installation des agents :
- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
  - Dans le volet de navigation, choisissez **Manage > Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).
- Étape 2** Cliquez sur **Agent Script Installer** (Installateur de script d'agent).
- Étape 3** Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez **Windows**.  
Pour afficher les plateformes Windows prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).
- Étape 4** Choisissez le détenteur pour installer les agents.
- Note** La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.
- Étape 5** Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.  
Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :
- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
  - Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.
- Étape 6** Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.
- Étape 7** Dans la section **Installer expiration** (Expiration de la validité de l'installateur), sélectionnez une option parmi celles disponibles :

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

**Étape 8**

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

**Étape 9**

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

**Note**

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

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

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

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

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

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

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

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



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

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

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

### Prérequis

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

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

### Procédure

#### Étape 1

Accédez à Méthodes d'installation des agents :

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

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

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

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

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

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

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

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

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

**Table 1: Options disponibles pour le programme d'installation MSI**

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

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

**Note**

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

## Vérifier l'installation de l'agent Windows

### Procédure

#### Étape 1

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

#### Étape 2

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

Exécutez la commande `sc query tetsensor sc query cswagent`

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

Exécuter la commande `sc qc tetsensorsc qc cswagent`

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

OU

Exécutez la commande `services.msc`

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

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

---

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

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

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

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

Exécuter la commande `sc qc tetsensorsc qc cswagent`

Cochez SERVICE\_START\_NAME.<utilisateur du service configuré>

Exécutez la commande `sc qc tetenforcer`

Cochez SERVICE\_START\_NAME.<utilisateur du service configuré>

OU

Exécutez la commande `services.msc`

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

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

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

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

OU

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

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

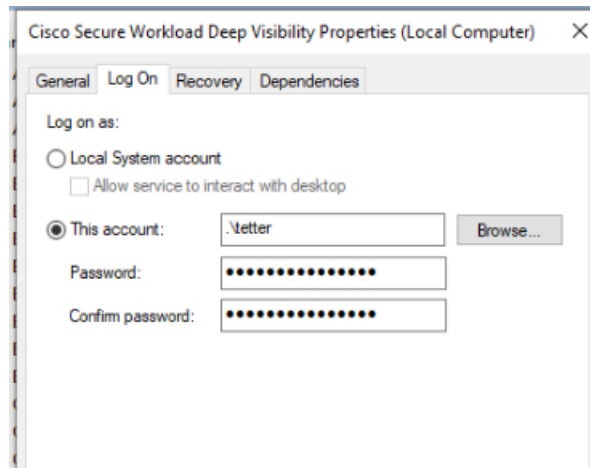
Vérifier le contexte utilisateur pour les processus en cours d'exécution (5e colonne)

## Modifier le compte de service

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

- Utilisez `services.msc`.

Illustration 3 : Modifier le compte de service en fonction du compte services.msc



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



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

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

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

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

#### Procédure

- 
- Étape 1** Installez l'agent sur une image idéale dans un environnement VDI ou un modèle de machine virtuelle à l'aide d'un programme d'installation MSI ou d'un script d'installation PowerShell :
- Utiliser le programme d'installation MSI avec **nostart=yes**
- Pour en savoir plus, consultez [Installer l'agent Windows à l'aide de la méthode du programme d'installation de l'image de l'agent, on page 12](#).
  - `msiexec.exe /<MSI installer> nostart="yes" /quiet /norestart /!*v <installer_log_file>` OU
- OU
- Utilisez le programme d'installation PowerShell avec l'indicateur **-goldenImage**.
- Pour en savoir plus, consultez [Installer l'agent Windows à l'aide de la méthode du programme d'installation du script de l'agent, on page 10](#).
- Étape 2** Vérifiez que le dossier `C:\Program Files\Cisco Tetration` (ou le dossier personnalisé) existe.
- Étape 3** Assurez-vous que le service TetSensor (pour une visibilité approfondie) existe et qu'il est arrêté :
- Exécutez la commande `cmd.exe` avec des privilèges d' **administrateur**.
- Exécutez la commande `sc query tetsensor`.
- Vérifiez si STATE (ÉTAT) est **arrêté**.
- Étape 4** Assurez-vous que le service TetEnforcer (pour la mise en application) existe et qu'il est arrêté :
- Exécutez la commande `sc query tetenforcer`.
- Vérifiez si STATE (ÉTAT) est arrêté.
- .
- Étape 5** Vérifiez que le service CswAgent existe et qu'il est arrêté :
- Exécutez la commande `cmd.exe` avec des privilèges d' **administrateur**.
- Exécutez la commande `sc query cswagent`
- Vérifiez si STATE (ÉTAT) est **arrêté**.
- Étape 6** Le modèle de machine virtuelle est maintenant configuré.

**Étape 7** Arrêtez le modèle de machine virtuelle.

---

## Créer une nouvelle instance de machine virtuelle VDI

### Procédure

---

- Étape 1** Créez une nouvelle machine virtuelle d'instance VDI en dupliquant le modèle de machine virtuelle.
- Étape 2** Redémarrez la machine virtuelle de l'instance VDI.
- Étape 3** Après avoir redémarré la machine virtuelle de l'instance VDI, assurez-vous que les services – TetSensor (pour une visibilité approfondie) et TetEnforcer (pour l'application) – s'exécutent dans le contexte de service configuré. Reportez-vous à la section [Vérifier l'installation de l'agent Windows](#).
- Étape 4** Après avoir redémarré la machine virtuelle de l'instance VDI, vérifiez que le service CswAgent est en cours d'exécution dans le contexte de service configuré. Reportez-vous à la section [Vérifier l'installation de l'agent Windows](#).
- Étape 5** Sur la machine virtuelle de l'instance VDI, assurez-vous que le pilote NPCAP est installé et en cours d'exécution :
- Exécutez la commande `cmd.exe` avec des privilèges d'administrateur.
- Exécutez la commande `sc query npcap`
- Vérifiez si STATE (ÉTAT ) est égal à **Running** (Exécution en cours)
- Étape 6** Sur la machine virtuelle de l'instance VDI, assurez-vous que l'agent est enregistré à l'aide d'un `sensor_id` (identifiant de capteur) valide :
- Vérifiez le fichier `Sensor_id` dans le dossier d'installation.
  - Si `sensor_id` commence par « uuid », il ne s'agit pas d'un `sensor_id` valide.
  - Si l'agent ne s'enregistre pas, mais que l'interface Web Cisco Secure Workload indique que l'agent est enregistré :
  - Supprimez l'agent à l'aide d'OpenAPI. Pour en savoir plus, consultez la section [Déployer des agents logiciels](#).
- Note**
- Ne modifiez pas le nom d'hôte de l'image golden (idéale) ou du modèle de machine virtuelle.
  - Si l'image idéale ou le modèle de machine virtuelle est redémarré après l'installation de l'agent, les services Cisco Secure Workload commencent à s'exécuter après le redémarrage.
  - Si la machine virtuelle de l'instance VDI ne signale pas les flux de réseau, consultez la section *Machine virtuelle de l'instance VDI dans les flux réseau*.
- 

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

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

## 2. Installation :

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

## 3. Mettre à niveau :

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

## 4. Désinstaller :

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

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

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

Lors de la mise à jour vers la dernière version :

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

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



### Note

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

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



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

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

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

- Toutes les fonctions de visibilité approfondie ne sont pas prises en charge dans AIX. La comptabilité des paquets et des processus fait partie de celles qui ne sont pas prises en charge.
- Exigences supplémentaires pour l'application des politiques :
  - Si le filtre de sécurité IP est activé (c'est-à-dire, smitty IPsec4), l'installation de l'agent échoue lors de la vérification préalable. Nous vous recommandons de désactiver le filtre de sécurité IP avant d'installer l'agent.
  - Si la sécurité IP est activée lorsque l'agent de mise en application de Cisco Secure Workload est en cours d'exécution, une erreur est signalée et l'agent d'application arrête l'application de la politique. Communiquez avec le service d'assistance pour désactiver en toute sécurité le filtre de sécurité IP lorsque l'agent de mise en application est en cours d'exécution.

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

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



### Note

- L'agent AIX installé prend en charge la visibilité approfondie et l'application.
- Le paramètre par défaut est Disabled (désactivé). Pour activer l'application, consultez [Creating an Agent Config Profile, on page 65](#).

Pour installer un agent AIX :

### Procédure

#### Étape 1

Accédez à Méthodes d'installation des agents :

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

#### Étape 2

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

#### Étape 3

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

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

#### Étape 4

Choisissez le détenteur pour installer les agents.

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

#### Étape 5

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

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

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

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

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

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

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

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

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

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

**Étape 11** Pour installer l'agent, exécutez la commande suivante avec les privilèges racine :

`./tetration_installer_default_sensor_aix.sh`

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

---

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

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

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

```

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

```

## Vérifier l'installation de l'agent AIX

### Procédure

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

**Remarque** La sortie spécifique peut différer selon la version

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

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

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

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

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

---

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

## Requirements and Prerequisites

### Kubernetes 1.[16-22]

- RHEL: 7.[0-9] (only x86\_64 architecture)
- CentOS: 7.[0-8] (only x86\_64 architecture)
- Oracle Linux: 7.[0-8] (only x86\_64 architecture)
- Ubuntu: 16.04, 18.04, 20.04 (only x86\_64 architecture)
- SUSE Linux Enterprise Server: 12sp[0-5] (only x86\_64 architecture)
- Amazon Linux 2 (only x86\_64 architecture)

### Openshift 4.[5-9]

- Red Hat Enterprise Linux CoreOS: 4.[5-9] (only x86\_64 architecture)

### Container Runtime

- Docker
- CRI-O
- containerd ( $\geq 1.5.x$ )



---

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

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

Restart the containerd daemon.

---

### Additional Requirements

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



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

### Requirements for Policy Enforcement

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

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

These agents should be configured with the Preserve Rules option enabled. See [Creating an Agent Config Profile](#).

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

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

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

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

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

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



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

### Procedure

#### Étape 1

Accédez aux méthodes d'installation des agents :

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

#### Étape 2

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

- Étape 3** Dans le menu déroulant **Select Platform** (Sélectionner une plateforme), choisissez **Kubernetes**.  
Pour afficher les plateformes Kubernetes ou OpenShift prises en charge, cliquez sur **Show Supported Platforms**(afficher les plateformes prises en charge).
- Étape 4** Choisissez le détenteur pour installer les agents.
- Note** La sélection d'un détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.
- Étape 5** Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes(Oui)**, puis saisissez une URL de serveur mandataire valide.
- Étape 6** Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.
- Étape 7** Exécutez le script d'installation sur une machine Linux qui a accès au serveur d'API Kubernetes et à un fichier de configuration kubectl avec des privilèges d'administration comme contexte/grappe/utilisateur par défaut.  
Le programme d'installation tente de lire le fichier à partir de son emplacement par défaut (~/.kube/config). Cependant, vous pouvez spécifier explicitement l'emplacement du fichier de configuration à l'aide de la commande --kubeconfig.

---

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




---

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

---

## Installation des agents Solaris pour une visibilité approfondie

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

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

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

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

### Procédure

- Étape 1** Accédez à Méthodes d'installation des agents :
- Si vous utilisez le logiciel pour la première fois, lancez l'assistant de démarrage rapide et cliquez sur **Install Agents** (Installer les agents).
  - Dans le volet de navigation, choisissez **Manage > Agents**(Gestion > Agents), puis sélectionnez l'onglet **Installer** (Installateur).
- Étape 2** Cliquez sur **Agent Script Installer** (Installateur de script d'agent).
- Étape 3** Dans le menu déroulant **Select Platform** (sélectionner une plateforme), choisissez « **Solaris** ».
- Pour afficher les plateformes Solaris prises en charge, cliquez sur **Show Supported Platforms**(Afficher les plateformes prises en charge).
- Étape 4** Choisissez le détenteur pour installer les agents.
- Note** La sélection du détenteur n'est pas requise pour les grappes de logiciel-service Cisco Secure Workload.
- Étape 5** Si vous souhaitez attribuer des étiquettes à la charge de travail, choisissez les clés d'étiquette et saisissez les valeurs d'étiquette.
- Lorsque l'agent installé signale des adresses IP sur l'hôte, les étiquettes CMDB de l'installateur sélectionnées ici, ainsi que les autres étiquettes CMDB téléversées qui ont été attribuées aux adresses IP signalées par cet hôte, sont automatiquement attribuées à la nouvelle adresse IP. En cas de conflit entre les étiquettes de la CMDB téléversées et celles de la CMDB d'installation :
- Les étiquettes attribuées à une adresse IP exacte prévalent sur les étiquettes attribuées au sous-réseau.
  - Les étiquettes existantes attribuées à une adresse IP exacte prévalent sur les étiquettes de la CMDB d'installation.
- Étape 6** Si un serveur mandataire HTTP est requis pour communiquer avec Cisco Secure Workload, choisissez **Yes**(Oui), puis saisissez une URL de serveur mandataire valide.
- Étape 7** Dans la section **Installer expiration** (Expiration de la validité de l'installateur), sélectionnez une option parmi celles disponibles :
- Aucune expiration : le script d'installation peut être utilisé plusieurs fois.
  - Une fois : le script d'installation ne peut être utilisé qu'une seule fois.
  - Limité dans le temps : vous pouvez définir le nombre de jours pendant lesquels le script d'installation peut être utilisé.
  - Nombre de déploiements : vous pouvez définir le nombre d'utilisations du script d'installation.
- Étape 8** Cliquez sur **Download** (Télécharger) et enregistrez le fichier sur le disque local.

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

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

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

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

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

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

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

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

## Vérifier l'installation de l'agent Solaris

### Procédure

#### Étape 1

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

#### Étape 2

Une seule entrée constituant la sortie confirme qu'un agent Solaris est installé sur l'hôte.

Exemple de sortie :

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

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

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

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

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

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



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

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

### Procédure

#### Étape 1

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

- Étape 2** Ouvrez le fichier `user.cfg` dans le dossier d'installation de l'agent Cisco Secure Workload. (Exemple : `/usr/local/tet` sous Linux ou `C:\Program Files\Cisco Tetration` sous Windows). Le fichier contient une liste de variables sous la forme « clé=valeur », une sur chaque ligne.
- Étape 3** Ajoutez la clé d'activation à la variable **ACTIVATION\_KEY**. Exemple :  
`ACTIVATION_KEY=7752163c635ef62e6568e9e852d07bd21bfd60d0`
- Étape 4** Si l'agent nécessite un serveur mandataire HTTPS, ajoutez le serveur mandataire du protocole **http** et le port à l'aide de la variable **HTTPS\_PROXY**. Exemple : `HTTPS_PROXY=http://proxy.my-company.com:80`
- 

## Other Agent-Like Tools

### AnyConnect agents

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

For Windows, Mac, or Linux platforms, please refer to [Cisco AnyConnect Secure Mobility Client Data Sheet](#).

### ISE agents

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

### SPAN agents

SPAN agents work with the ERSPAN connector. For information, see [ERSPAN Connector](#).

### Integration with third-party and additional Cisco products

- Integrations using external orchestrators configured in Cisco Secure Workload.  
See [Orchestrateurs externes dans Cisco Secure Workload](#).
- Integrations using connectors configured in Cisco Secure Workload.  
See [What are Connectors](#).

## Renseignements sur la connectivité

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

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

Table 2: Connectivité des agents

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

Légende :

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

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

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



**Note**

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

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

## Exclusions de sécurité

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

**Table 3: Exclusions de sécurité pour les répertoires d'agents**

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

**Table 4: Exclusions de sécurité pour les processus d'agent**

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

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

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



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

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

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

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

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

Table 8: Exclusions de sécurité pour les actions des agents

Système d'exploitation de l'hôte	Actions
AIX	Access /dev/bpf*, /dev/ip1, /dev/kmem
	Invokes cfg_ipf, curl, ipf, ippool, ipfstat lspp, lsfilt, prtconf
	Scan /proc
Linux	Invokes curl, ip[6]tables-save, ip[6]tables-restore, rpm/dpkg
	Scan /proc, open netlink sockets
Windows	Accéder au registre
	S'inscrire aux événements du pare-feu
	Invokes c:\windows\system32\netsh.exe
Solaris	Invokes curl, lspp, pkg, smbios
	Scan /proc

Table 9: Exclusions de sécurité pour les scripts d'agent ou les exécutions binaires

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

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

## Gestion des services des agents

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



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

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

Exécutez les commandes suivantes pour :

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

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

Les commandes sont également applicables à :

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

Exécutez les commandes suivantes pour :

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

## Gestion des services pour Windows Server ou Windows VDI

Exécutez les commandes suivantes pour :

- **Démarrage d'un service** : `net start <nom du service>`  
 Exemple : **net start tetsensor** pour le service de visibilité approfondie - **net start tetenforcer** pour le service d'application  
 Exemple : **net start cswagent** pour le service de visibilité approfondie et d'application
- **Arrêter un service** : `net stop <nom du service>`  
 Exemple : **net stop tetsensor** pour le service de visibilité approfondie - **net stop tetenforcer** pour le service de mise en application  
 Exemple : **net stop cswagent** pour une visibilité approfondie et le service d'application
- **Redémarrage d'un service** :
  1. `net stop <nom du service>`
  2. `net start <nom du service>`
- **Vérification de l'état du service** : `sc query <nom du service>`  
 Exemple : **sc query tetsensor** pour le service de visibilité approfondie - **sc query tetenforcer** pour le service de mise en application  
 Exemple : **sc query cswagent** pour un service de visibilité approfondie et d'application

## Gestion des services pour AIX

Exécutez les commandes suivantes pour :

- **Démarrage d'un service** : `startsrc -s csw-agent`
- **Arrêt d'un service** : `stopsrc -s csw-agent`
- **Redémarrage d'un service** :
  1. `stopsrc -s csw-agent`
  2. `startsrc -s csw-agent`
- **Vérification de l'état du service** : `lssrc -s csw-agent`

## Gestion du service pour les installations d'agents Kubernetes

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

## Gestion des services pour Solaris

Exécutez les commandes suivantes pour :

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

## Application des politiques par le biais d'agents

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

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

### Mise en application utilisant des agents

- Les agents reçoivent les politiques sur un canal TCP ou SSL sécurisé.
- Les agents s'exécutent dans un domaine privilégié. Sur les machines Linux, l'agent s'exécute en tant qu'utilisateur « root »; sur les machines Windows, l'agent s'exécute en tant que SYSTEM.
- Selon la plateforme, lorsque l'application des politiques est activée, les agents peuvent contrôler complètement le pare-feu ou utiliser les règles configurées existantes.
- Pour en savoir plus sur les options d'application et pour activer et configurer les agents afin d'appliquer les politiques, consultez [Creating an Agent Config Profile, on page 65](#).

### Détails avancés

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

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

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

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

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

## Application par les agents sur la plateforme Linux

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

### iptables ou ip6tables Linux

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

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

Voici un exemple illustrant ce comportement :

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

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

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

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

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

## Mises en garde

### Module de noyau ipset

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

### Sauvegarde du pare-feu de l'hôte

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

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

## Application par les agents sur la plateforme Windows en mode WAF

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

### Pare-feu Windows avec sécurité avancée

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

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

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

## Règles Cisco Secure Workload et pare-feu Windows

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

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

## Profils de sécurité

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

- Profil de domaine
- Profil privé
- Profil public

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

## Politiques de paramètres et de listes mixtes en vigueur

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

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

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

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



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

Par exemple :

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

### Interférence provenant d'autres pare-feu ou politiques

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

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

## Application par état

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

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

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



---

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

---

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

## Mises en garde

### Sauvegarde du pare-feu de l'hôte

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

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

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

### Plateforme de filtrage Windows

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

### Avantages de WFP par rapport à WAF

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

### Prise en charge des agents pour WFP

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

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

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

Pour la politique du trafic entrant TCP,

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

les filtres WFP configurés sont les suivants :

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

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

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

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

## Politiques de paramètres et de listes mixtes en vigueur

La mise en application des agents en mode WFP prend en charge les politiques de listes mixtes ou grisées. Prenons l'exemple de la politique de liste mixte (autorisation et refus) de la section sur l'agent d'application :

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

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

## Application par état

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

## Visibilité des filtres WFP configurés

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

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

OU

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

## Désactiver les filtres du mode furtif en mode WFP

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

### Procédure

- 
- Étape 1** Modifiez `\conf\enforcer.cfg`.
- Étape 2** Ajoutez **`disable_wfp_stealth_mode: 1`**
- Étape 3** Enregistrez le fichier.
- Étape 4** Avec des privilèges d'administration, redémarrez le service `tetenforcer` en :
- Exécutant la commande : `sc stop tetenforcer to stop TetEnforcer Service.`
  - Exécutant la commande : `sc start tetenforcer to start TetEnforcer Service.`
- Étape 5** Avec des privilèges d'administration, redémarrez le service `CswAgent` en :
- Exécutant la commande : `sc stop cswagent pour arrêter le service CswAgent.`
  - Exécutant la commande : `sc start cswagent pour démarrer le service CswAgent.`
- Étape 6** Pour vérifier :
- Avec des privilèges d'administration, exécutez `cmd.exe`.
  - Exécutant la commande : `c:\program files\tetration\tetenf.exe -l -f <-verbose> <-output=outfile.txt>`.
-

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

## Supprimer les filtres WFP configurés

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

Les options prises en charge sont les suivantes :

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

## Limites connues du mode WFP

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

## Configurer les politiques pour les attributs Windows

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

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

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

### Avant de commencer

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

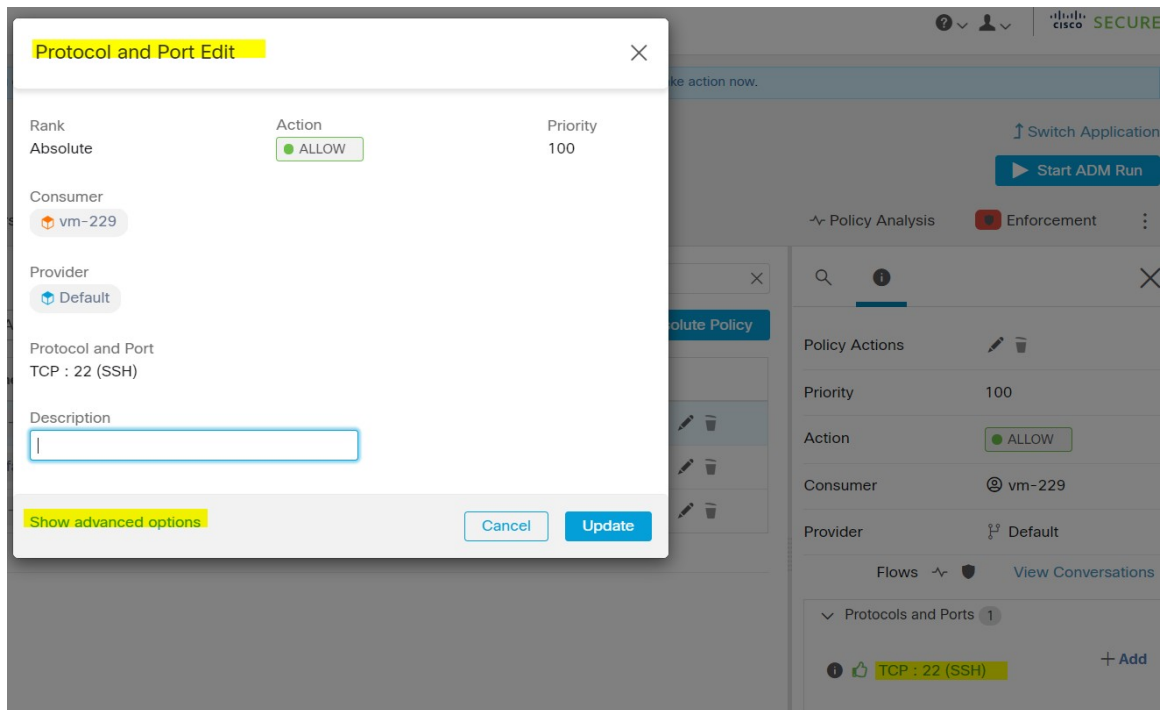


#### Important

Consultez [Mises en garde, à la page 49](#) et [Limites connues, à la page 48](#) pour des renseignements sur les politiques impliquant les attributs Windows.

## Procédure

- Étape 1** Dans le volet de navigation, cliquez sur **Defend (Défendre) > Segmentation**.
- Étape 2** Cliquez sur la portée qui contient la politique pour laquelle vous souhaitez configurer des filtres basés sur le système d'exploitation Windows.
- Étape 3** Cliquez sur l'espace de travail dans lequel vous souhaitez modifier la politique.
- Étape 4** Cliquez sur **Manage Policies** (Gestion des politiques).
- Étape 5** Choisissez la politique à modifier.
- Important** Le client et le fournisseur doivent inclure uniquement les charges de travail Windows.
- Étape 6** Dans la ligne du tableau permettant de modifier la politique, cliquez sur la valeur existante dans la colonne **Protocols and Ports** (protocoles et ports).
- Étape 7** Dans le volet de droite, cliquez sur la valeur existante sous **Protocols and Ports**.  
Dans l'exemple, cliquez sur **TCP : 22 (SSH)**.



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

While using process level controls a consumer/provider scope or filter should only contain Windows agents. Otherwise, non-Windows OSs (Linux, AIX) will skip the policy and report a sync error in Enforcement Status. See the user guide for more information.

Consumer Service

Consumer Binary Path

Consumer Users or User Groups ⓘ

Provider Service

Provider Binary Path

Provider Users or User Groups ⓘ

[Hide advanced options](#)

**Étape 9**

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

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

**Étape 10**

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

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

**Étape 11**

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

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

**Étape 12**

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

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

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

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

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

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

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

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

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

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

### Limites connues

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



## Mises en garde

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

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

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

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

### Politiques basées sur le nom de l'application

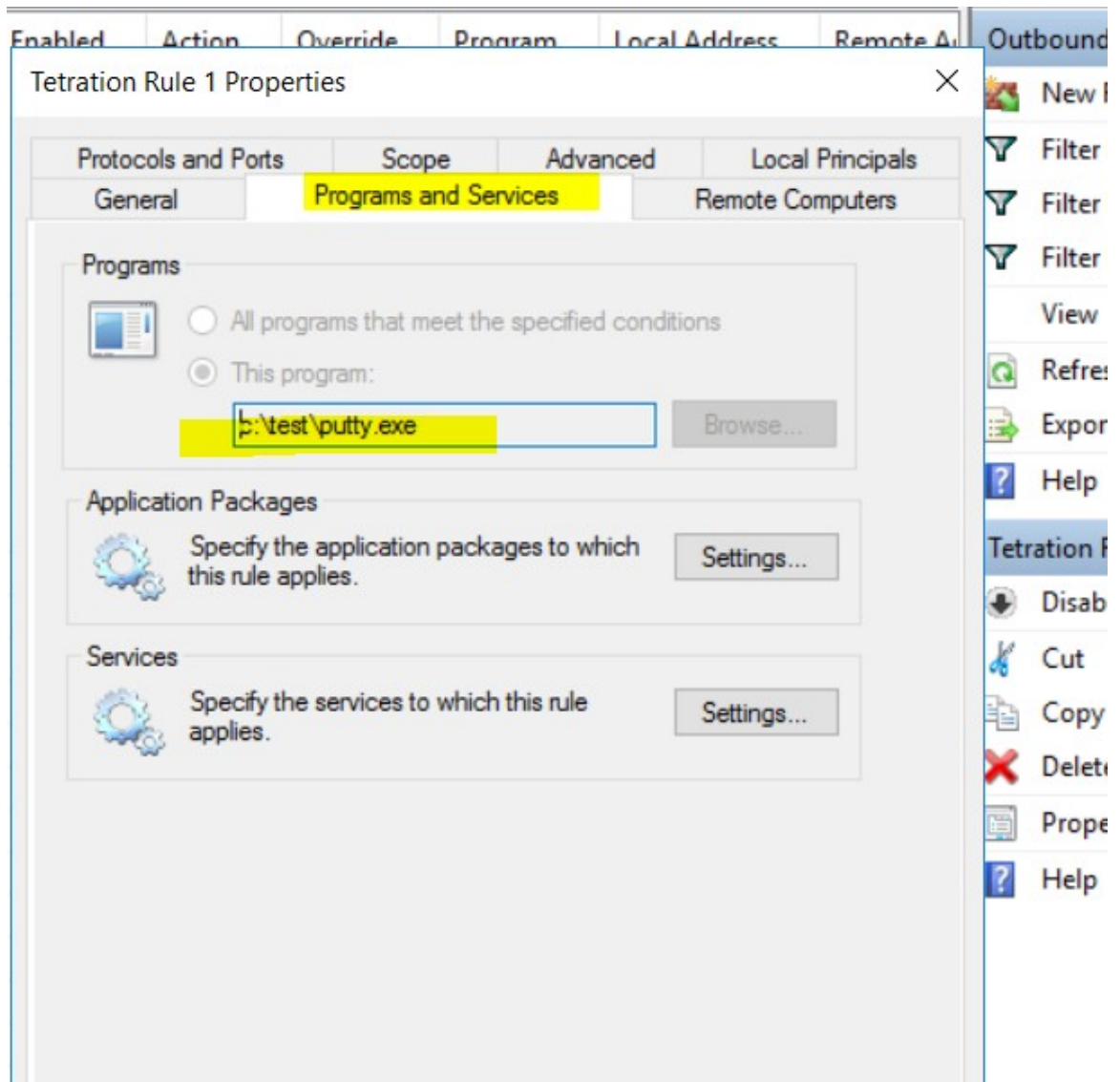
Utilisez les informations suivantes pour vérifier et dépanner les politiques en fonction du nom de l'application sur les charges de travail avec système d'exploitation Windows.

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

#### Exemple de politique basée sur le nom de l'application

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

### Règle de pare-feu générée



### Filtre généré à l'aide de netsh

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

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

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

```

        <type>FWP_BYTE_BLOB_TYPE</type>
        <byteBlob>
            <data>
                ↪5c006400650076006900630065005c0068006100720064006400690073006b0076006f006
            ↪</data>
                <asString>\device\harddiskvolume2\temp\putty.exe</
            ↪asString>
        </byteBlob>
    </conditionValue>

```

### \_filtre WFP généré à l'aide de tetenf.exe -l -f

```

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

```

### Nom d'application non valide

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

## Politiques basées sur le nom du service

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

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

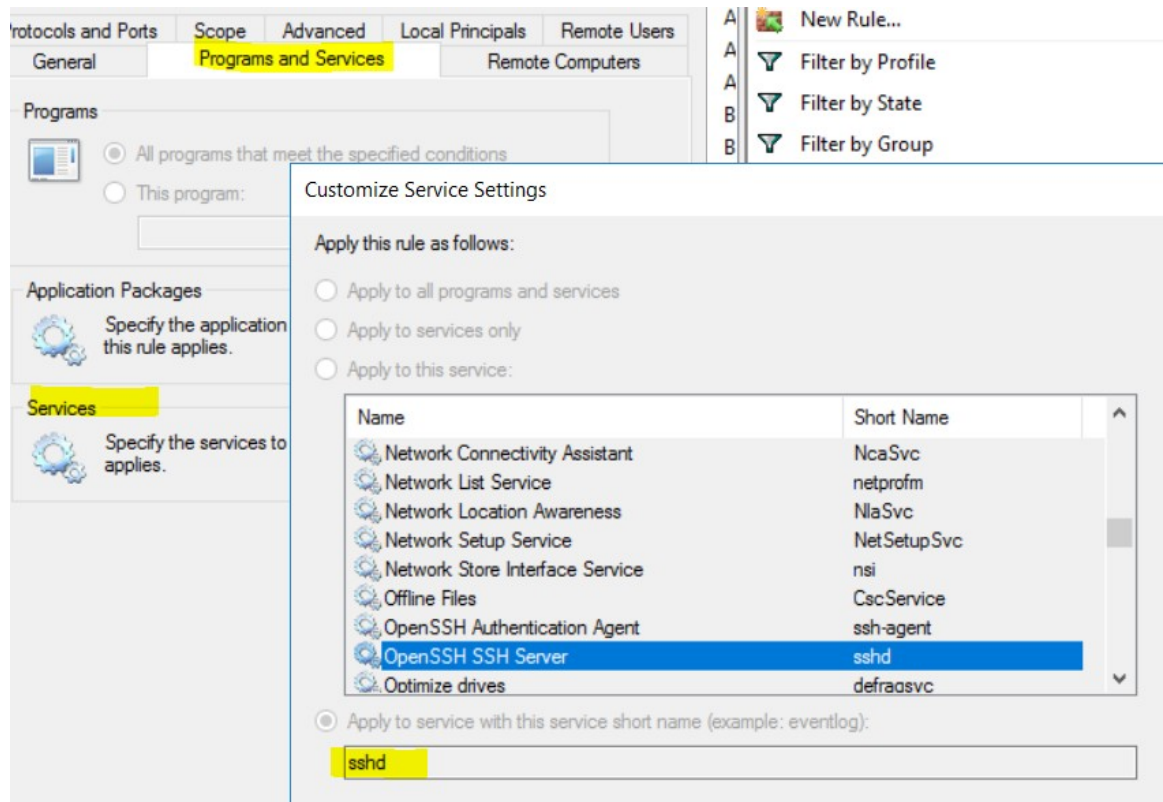
### Exemple de politique basée sur le nom de service

```

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

```

## Règle de pare-feu générée



## Filtre généré à l'aide de netsh

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

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

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

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

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

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

### Nom non valide

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

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

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

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

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

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

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

Figure 4: Politiques basées sur le groupe d'utilisateurs ou le nom d'utilisateur

Description

While using process level controls, a consumer/provider scope or filter should only contain Windows agents. Otherwise, non-Windows OSs (Linux, AIX) will skip the policy and report a sync error in Enforcement Status. See the user guide for more information.

Consumer Service

Consumer Binary Path

Consumer Users or User Groups ⓘ  
sensor-dev\domain users,sensor-dev@se

Provider Service

Provider Binary Path

Provider Users or User Groups ⓘ

### Exemple de politique basée sur le nom d'utilisateur

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

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

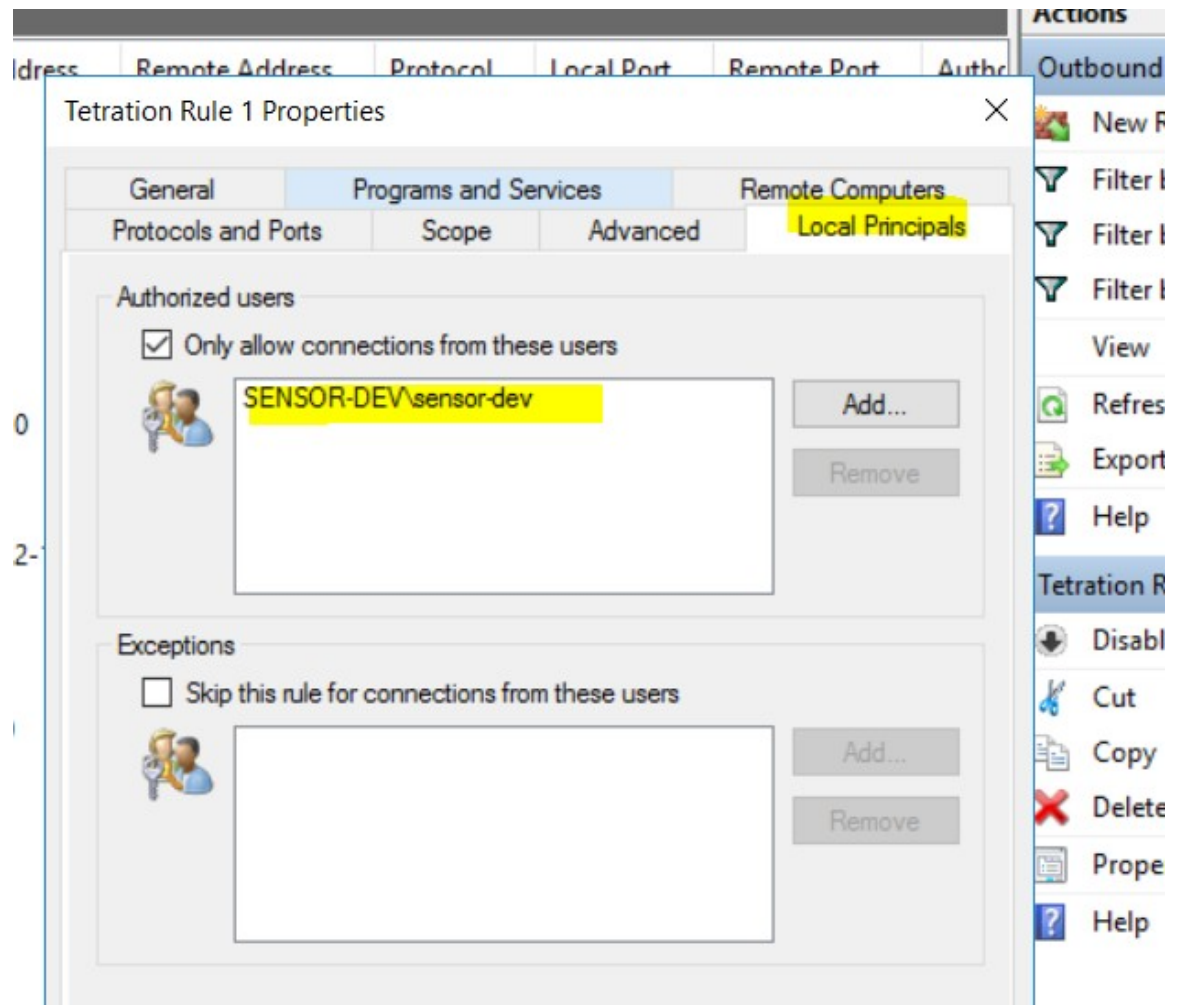
```
dst_ports {
  start_port: 30000
  end_port: 30000
  provider_filters {
    user_name: "sensor-dev\domain users,sensor-dev\sensor-dev"
  }
}
ip_protocol: TCP
```

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

### Règle de pare-feu générée

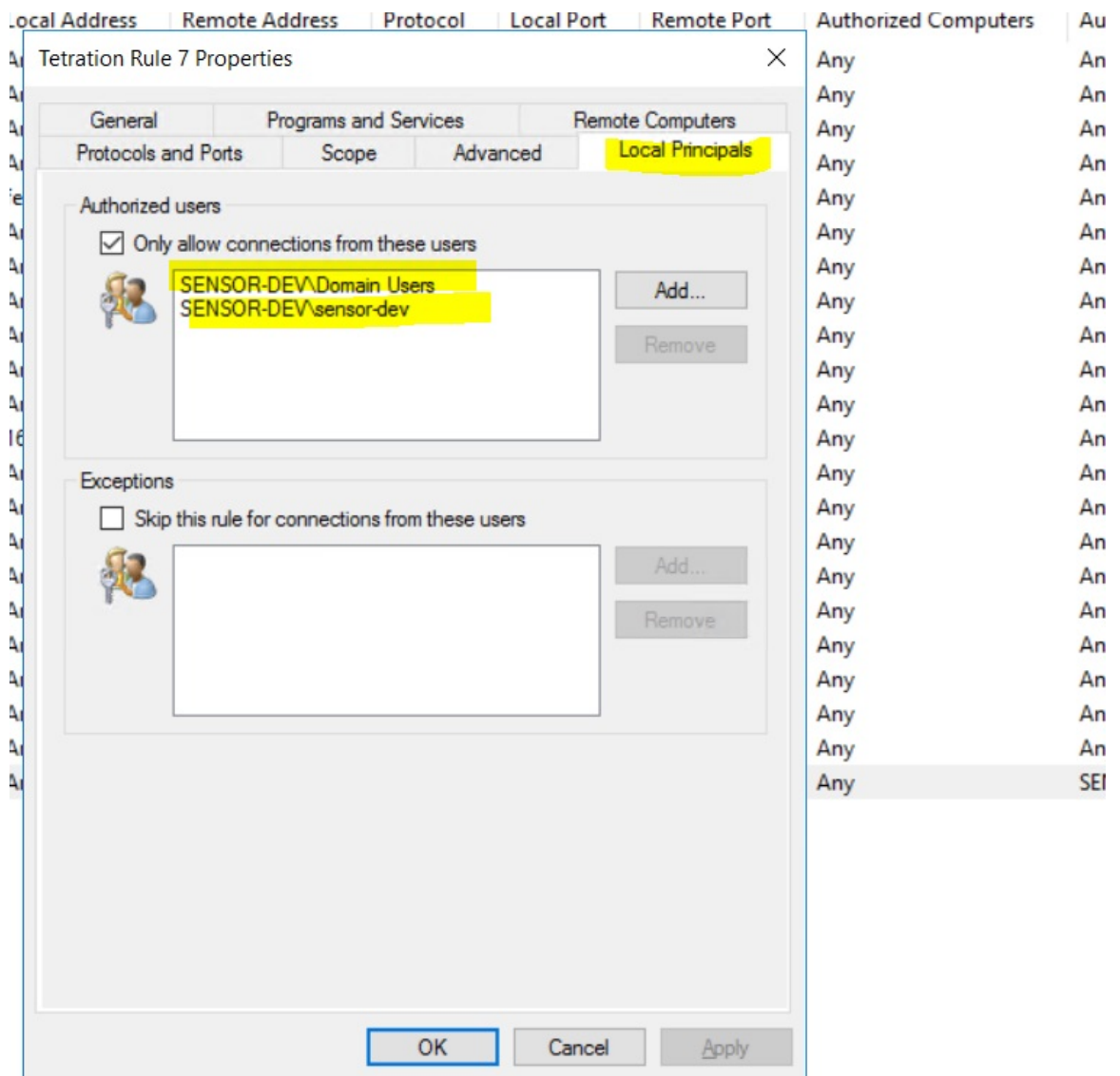
#### Règle de pare-feu basée sur le nom d'utilisateur

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



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

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



### Filtre généré à l'aide de netsh

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

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

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



```

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

```

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

#### Filtrer en fonction du nom d'utilisateur

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

```

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

```

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

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

```

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

```

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



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

## Application des Pods Kubernetes sur les nœuds Windows

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

### Exigences

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

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

Chaque filtre possède les attributs suivants :

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

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

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

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

### Compatibilité avec Calico

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




---

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

---

### Visibilité des filtres VFP configurés

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

### Supprimer les filtres VFP configurés par l'agent Windows

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



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

### Dépannage des politiques appliquées et des flux réseau

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

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

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

## Application des agents sur la plateforme AIX

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

### IPFilter

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

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

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

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

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

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

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

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

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

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

## Mises en garde

### Sauvegarde du pare-feu de l'hôte

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

## Limites connues

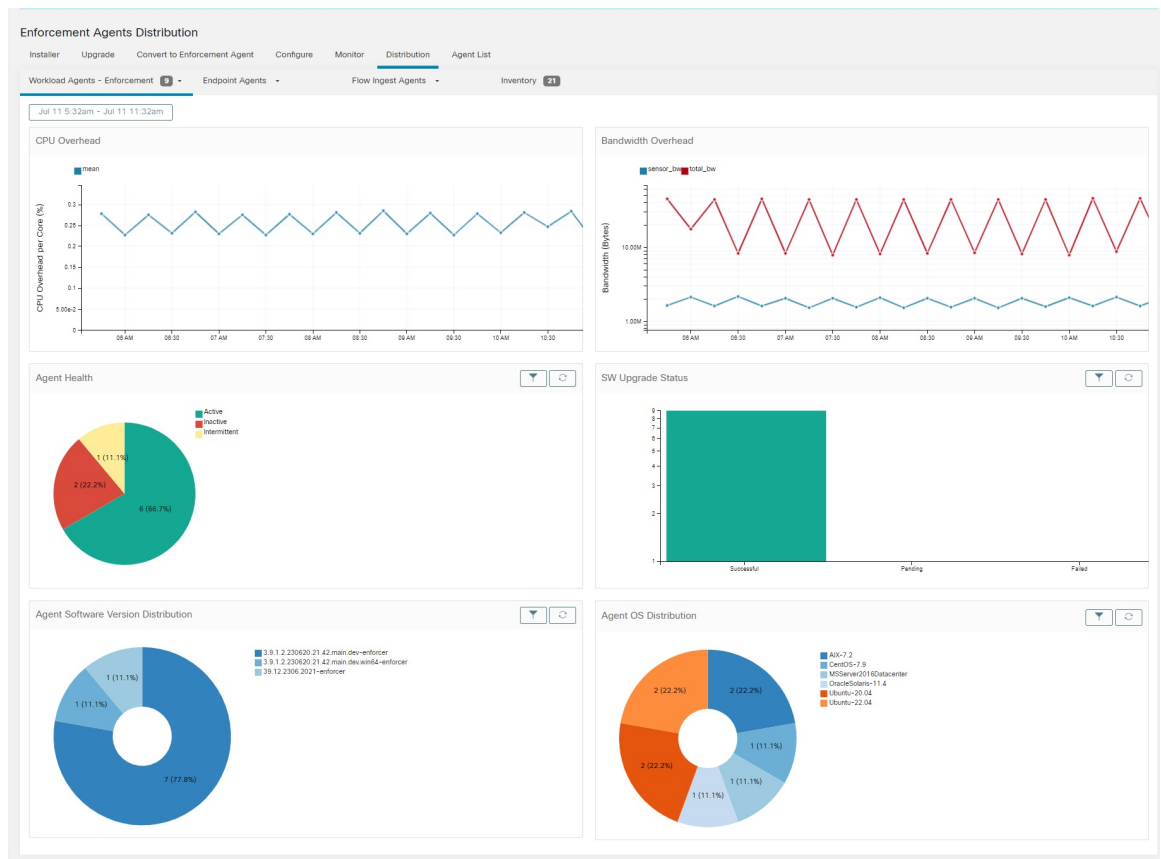
L'application de IPv6 n'est pas prise en charge.

# État et statistiques de l'agent

## Procédure

- Étape 1** Dans le volet de navigation, cliquez sur **Manage (Gestion) > Workloads (Charges de travail) > Agents (Agents)**.
- Étape 2** Cliquez sur l'onglet **Distribution (Répartition)**.
- Étape 3** Cliquez sur un type d'agent en haut de la page.
- Étape 4** Sur cette page, vous pouvez vérifier la surcharge du CPU, la surcharge de la bande passante, l'intégrité de l'agent, l'état des mises à jour logicielles, la répartition des versions du logiciel de l'agent et la répartition du système d'exploitation de l'agent.

**Figure 5: Page Répartition des agents**



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

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

## Afficher les détails de l'agent

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

### Procédure

- 
- |                |  |
|----------------|--|
| <b>Étape 1</b> | Dans le menu de navigation, cliquez sur <b>Organize &gt; &gt; Scopes and Inventory</b> (Organiser > Portées et inventaire).  |
| <b>Étape 2</b> | Recherchez une charge de travail pour laquelle vous souhaitez afficher les détails.  |
| <b>Étape 3</b> | Cliquez sur l'adresse IP pour afficher des détails tels que l'intégrité de l'agent, l'adresse IP, la portée, le type d'inventaire, les groupes d'application, les groupes expérimentaux, les étiquettes d'utilisateur et le volume de trafic (total des octets/total des paquets). |
- 

Pour en savoir plus, consultez [Profil de la charge de travail](#).

## Configuration de l'agent logiciel

### Exigences et conditions préalables à la configuration des agents logiciels

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

Pour en savoir plus, consultez [Rôles des utilisateurs et accès à la configuration des agents, on page 62](#).

- Assurez-vous de disposer des privilèges sur l'hôte pour exécuter le service d'agent sur chaque charge de travail. Pour en savoir plus, consultez la section [Gestion des services des agents](#).
- Vérifier les plateformes prises en charge, la configuration requise et les instructions d'installation pour les agents. Pour en savoir plus, consultez la section [Déployer des agents logiciels](#).

### Rôles des utilisateurs et accès à la configuration des agents

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



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

**Figure 6: Configuration d'agent logiciel pour les propriétaires de portée**

The screenshot displays the 'Agent Config Profiles' and 'Agent Config Intents' sections. The 'Agent Config Profiles' table shows a 'Default' profile with various configuration options like 'Enforcement', 'Flow Visibility', and 'Process Visibility and Forensics'. The 'Agent Config Intents' section shows three categories: 'Apply profile Default to filter Everything', 'Interface Config Intents' (No intents found), and 'Agent Remote VRF Configurations' (No configs found).

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

## Configurer les agents logiciels

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



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

Figure 7: Configuration de l'agent logiciel

Software Agents Configure

Installer Upgrade Convert to Enforcement Agent **Configure** Monitor Distribution Agent List

Agent Config Profiles Create Profile

Name	Config	Actions
Default	<ul style="list-style-type: none"> <li>Enforcement                             <ul style="list-style-type: none"> <li>● Enforcement</li> <li>● Windows Enforcement Mode - WFP</li> <li>● Preserve Rules</li> <li>● Allow Broadcast</li> <li>● Allow Multicast</li> <li>● Allow Link Local Addresses</li> <li>● CPU Quota Mode - Adjusted (6%)</li> <li>● Memory Quota Limit - 512MB</li> </ul> </li> <li>Flow Visibility                             <ul style="list-style-type: none"> <li>● Flow Analysis Fidelity - Detailed</li> <li>● Data Plane</li> <li>● Auto-Upgrade</li> <li>● PID/User Lookup</li> <li>● Service Protection</li> <li>● CPU Quota Mode - Adjusted (6%)</li> <li>● Memory Quota Limit - 512MB</li> <li>● Cleanup Period - 1d</li> <li>● Flows Disk Quota - 512MB</li> </ul> </li> <li>Process Visibility and Forensics                             <ul style="list-style-type: none"> <li>● Forensics</li> <li>● Process Visibility</li> <li>● Package Visibility</li> <li>● Meltdown Exploit Detection</li> <li>● CPU Quota Mode - Adjusted (6%)</li> <li>● Memory Quota Limit - 768MB</li> </ul> </li> </ul>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Edit</div> <span>⋮</span> Used by 1 Intent

Agent Config Intents Create Intent

Apply profile Default to filter **Everything**

[View Deleted Agent Config Intents](#) ⋮

Interface Config Intents Create Intent

No intents found

Agent Remote VRF Configurations Create Config

No configs found



Figure 8: Configuration de l'agent logiciel

## Creating an Agent Config Profile

### Before you begin

See [Exigences et conditions préalables à la configuration des agents logiciels](#), on page 62.

### Procedure

- Étape 1** In the navigation bar on the left, click **Manage > Agents**.
- Étape 2** Click the **Configure** tab.
- Étape 3** Click the **Create Profile** button.
- Étape 4** Enter a name for the profile (required) and select a scope where profile will be available.
- Étape 5** Enter the appropriate values in the fields listed in the tables below:

Table 10: Enforcement config

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

Option	Description
<b>Memory Quota Limit (MB)</b>	Specify the memory limit in MB that the process is allowed to use. If the process hits this limit, it will restart.
<b>Windows Enforcement Mode</b>	<p>On Windows workloads, agents can enforce network policies using:</p> <ul style="list-style-type: none"> <li>• <b>WFP</b> - Windows Filtering Platform (by directly programming WFP filters in the Windows Filter Engine.) See <a href="#">Mise en application par les agents sur la plateforme Windows en mode WFP, on page 42.</a></li> <li>• <b>WAF</b> (Default) - Windows Advanced Firewall. See <a href="#">Application par les agents sur la plateforme Windows en mode WAF, on page 39.</a></li> </ul>

Table 11: Flow Visibility config

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

Field	Description
<b>Service Protection</b>	<p><b>Enable</b> - Enable service protection on the agent. When enabled, the agent ensures it prevents users from disabling the service, from uninstalling the agent, and from restarting the service. However, once the service protection is disabled, users can continue to stop or uninstall the agent.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Do not disable service protection for normal auto upgrade of an agent.</li> <li>• Do not enable service protection for manual upgrade of an agent.</li> <li>• Service protection blocks any forced upgrades, such as using the installer script - forceUpgrade option.</li> <li>• Any system initiated upgrade works seamlessly when the service protection is enabled.</li> </ul> <p><b>Disable(*)</b>-By default, service protection is disabled on the agent.</p> <p><b>Detailed</b> (Default) - Enable detailed mode on all sensors.</p> <p><b>Note</b> This feature is available only for Windows agent.</p>
<b>CPU Quota Mode</b>	<p><b>Adjusted</b> (Default) - The CPU limit is adjusted according to the number of CPUs on the system. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system, selecting this mode means that agent is allowed to use a total of 30% (measured by top).</p> <p><b>Top</b>- The CPU limit value would match the top view on average. For example, if the CPU limit is set to 3% and there are 10 CPUs in the system. The cpu usage would still be 3%. This is a fairly restrictive mode and should be used only when necessary.</p> <p><b>Disable</b> - The CPU limit feature is disabled. The agent will use CPU resources permitted by the OS.</p> <p>See <a href="#">agent_cpu_sla.pdf</a> for more information.</p>
<b>CPU Quota Limit (%)</b>	Specify the actual limit in percentage of the system processing power the agent can use.
<b>Memory Quota Limit (MB)</b>	Specify the memory limit in MB that the process is allowed to use. If the process hits this limit, it will restart.
<b>Cleanup period (days)</b>	<p><b>Enable</b> - Enable automated cleanup on the agent. Enter the number of days after which the inactive agent is removed.</p> <p><b>Disable</b> (Default) - Do not enable automated cleanup on the agent.</p>
<b>Flow Analysis Fidelity</b>	<p><b>Conversations</b> - Enable conversations mode on all sensors.</p> <p><b>Detailed</b> (Default) - Enable detailed mode on all sensors</p>
<b>Flows Disk Quota (MB)</b>	Specify in MB the total size limit of stored flow data.

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

**Figure 9: Flow Visibility**

The screenshot shows a configuration page titled "Enforcement". It contains the following settings:

- Enforcement:**  Enable  Disable (Default)
- Windows Enforcement Mode:**  WAF  WFP (Default)
- Preserve Rules:**  Enable  Disable (Default)
- Allow Broadcast:**  Enable (Default)  Disable
- Allow Multicast:**  Enable (Default)  Disable
- Allow Link Local Addresses:**  Enable (Default)  Disable
- CPU Quota Mode:**  Disable  Adjusted (Default)  Top
- CPU Quota Limit (%):**
- Memory Quota Limit (MB):**

*Figure 10:*

Table 12: Process Visibility and Forensics Config

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

**Étape 6**

Click Save

**What to do next**

Associate this profile with an agent config intent. See [Création d'un intent de configuration d'agent](#), on page 72.

**Création d'un intent de configuration d'agent****Before you begin**

- Consultez [Exigences et conditions préalables à la configuration des agents logiciels](#), on page 62.
- Créez un profil de configuration d'agent. Consultez [Creating an Agent Config Profile](#), on page 65.

**Procedure**

- Étape 1** Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion) > Agents (Agents)**.
- Étape 2** Cliquez sur l'onglet **Configure** (Configurer).
- Étape 3** Cliquez sur le bouton **Create Intent** (créer un intent) à côté de l'en-tête de **l'intent de configuration de l'agent**.
- Étape 4** Saisissez les valeurs appropriées dans les champs répertoriés dans le tableau ci-dessous :

Champ	Description
<b>Profil</b> (obligatoire)	Saisissez le nom d'un profil existant et sélectionnez-le dans le menu déroulant.
<b>Filtre</b> (obligatoire)	Saisissez le nom d'un filtre existant ou de la portée, ou sélectionnez <i>Create new filter</i> (créer un filtre) dans le menu déroulant.  Consultez la section <a href="#">Filtres</a> pour en savoir plus sur la création de filtres.

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

**Figure 11: Intents de configuration de l'agent**

**Agent Config Intents**

Apply profile  to filter

Apply profile **Default** to filter [Everything](#)



## Création d'une configuration VRF distante pour les agents

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

### Procédure

- Étape 1** Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion) > Agents (Agents)**.
- Étape 2** Cliquez sur l'onglet **Configure** (Configurer).
- Étape 3** Cliquez sur le bouton **Create Config** (créer une configuration) à côté de l'en-tête **Agent Remote VRF Configurations** (Configurations VRF à distance de l'agent).
- Étape 4** Saisissez les valeurs appropriées dans les champs et cliquez sur **Save** (Enregistrer).

*Figure 12: Configuration VRF à distance*

### Agent Remote VRF Configurations

Apply VRF  
-----

Source Subnet  
10.1.0.0/16

Source Port Start  
0

Source Port End  
65535

Create Cancel

## Créer un intent de configuration d'interface

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

### Procédure

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

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

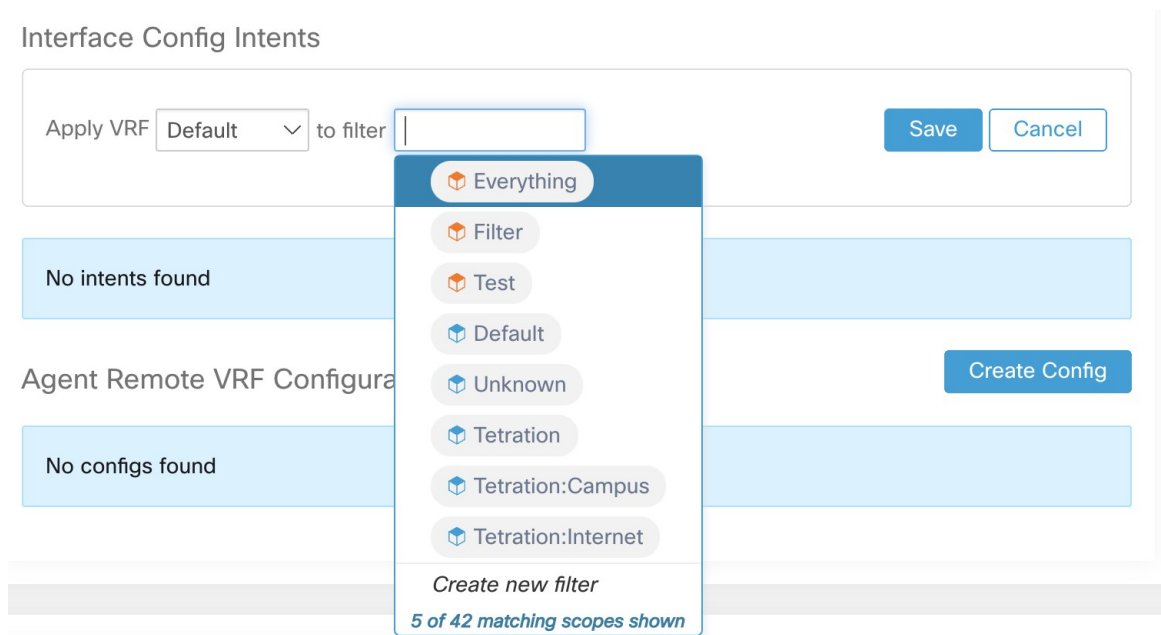
**Étape 3** Cliquez sur le bouton **Create Intent** (Créer un intent) à côté de l'en-tête **Interface Config Intent** (Intent de configuration d'interface).

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

Champ	Description
<b>VRF</b>	Choisissez un VRF dans la liste déroulante (obligatoire).
<b>Filter</b> (Filtrer)	Saisissez le nom d'un filtre existant ou d'une portée, ou sélectionnez <i>Create a new filter</i> (créer un filtre) dans la liste déroulante (obligatoire).  Pour en savoir plus, consultez <a href="#">Filtres</a> .

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

**Figure 13: Intents de configuration d'interface**



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

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

## Procédure

- Étape 1** Suivez les étapes ci-dessus pour vérifier l'état de l'agent.
- Étape 2** Dans la page Enforcement Agents (Agents d'application), cliquez sur **Agent OS Distribution**(Répartition des agents par SE). Sélectionnez un système d'exploitation et cliquez sur l'image du filtre dans le coin supérieur droit de la zone.
- Étape 3** Sur la page Software Agent List (Liste des agents logiciels), les agents sont répertoriés avec la distribution sélectionnée du système d'exploitation.
- Étape 4** Cliquez sur **Agent** (agent) pour obtenir les détails de l'agent, puis cliquez sur IP address (adresse IP). Dans la page Workload Profile (profil de charge de travail), vous pouvez afficher les détails du profil d'hôte, du profil d'agent et des détails propres à l'agent, comme la bande passante, les processus de longue durée, les paquets, l'instantané du processus, la configuration, les interfaces, les statistiques, les politiques, les politiques de conteneur, etc.
- Étape 5** Cliquez sur l'onglet **Config** pour voir la configuration sur l'hôte final.
- Étape 6** Cliquez sur l'onglet **Politiques** (Politiques) pour voir les politiques appliquées sur l'hôte final.

Figure 14: Profil de la charge de travail - Config

The screenshot shows the 'Config' tab in the Workload Profile interface. On the left, a sidebar lists various categories: LABELS AND SCOPES, AGENT HEALTH, LONG LIVED PROCESSES, PROCESS SNAPSHOTS, INTERFACES, PACKAGES, VULNERABILITIES, CONFIG (highlighted), STATS, ENFORCEMENT HEALTH, CONTAINER POLICIES, NETWORK ANOMALIES, FILE HASHES, and DOWNLOAD LOGS. The main content area is titled 'Config' and contains the following settings:

- Config Intent** (edit icon): Apply profile **enforcer** to filter **Enf-Workloads**
- Config Profile** (edit icon):
  - Enforcement**
    - Enforcement
    - Windows Enforcement Mode - WFP
    - Preserve Rules
    - Allow Broadcast
    - Allow Multicast
    - Allow Link Local Addresses
    - CPU Quota Mode - Adjusted (3%)
    - Memory Quota Limit - 512MB
  - Flow Visibility**
    - Flow Analysis Fidelity - Detailed
    - Data Plane
    - Auto-Upgrade
    - PID Lookup
    - CPU Quota Mode - Adjusted (3%)
    - Memory Quota Limit - 512MB
  - Process Visibility and Forensics**
    - Forensics
    - Meltdown Exploit Detection
    - CPU Quota Mode - Adjusted (3%)
    - Memory Quota Limit - 256MB

Figure 15: Profil de la charge de travail - Politiques

Priority ↑	Packets ↓	Bytes ↓	Actions ↓	Direction ↓	Family ↓	Proto ↓	Src Inventory ↓	Src Ports ↓	Dest Inventory ↓	Dest Ports ↓
1	N/A	N/A	ALLOW	INGRESS	IPv4	TCP	any	any	172.21.95.163/32	22
2	N/A	N/A	ALLOW	EGRESS	IPv4	TCP	172.21.95.163/32	22	any	any
3	N/A	N/A	ALLOW	INGRESS	IPv4	TCP	any	22	172.21.95.163/32	any
4	N/A	N/A	ALLOW	EGRESS	IPv4	TCP	172.21.95.163/32	any	any	22
5	N/A	N/A	ALLOW	INGRESS	IPv4	ST	ubunthosts	any	172.21.95.163/32	any
6	N/A	N/A	ALLOW	EGRESS	IPv4	ST	172.21.95.163/32	any	ubunthosts	any
7	N/A	N/A	ALLOW	INGRESS	IPv4	ST	ubunthosts	any	172.21.95.163/32	any
8	N/A	N/A	ALLOW	EGRESS	IPv4	ST	172.21.95.163/32	any	ubunthosts	any
9	N/A	N/A	ALLOW	INGRESS	IPv4	STP	ubunthosts	any	172.21.95.163/32	any
10	N/A	N/A	ALLOW	EGRESS	IPv4	STP	172.21.95.163/32	any	ubunthosts	any
11	N/A	N/A	ALLOW	INGRESS	IPv4	STP	ubunthosts	any	172.21.95.163/32	any
12	N/A	N/A	ALLOW	EGRESS	IPv4	STP	172.21.95.163/32	any	ubunthosts	any
13	N/A	N/A	ALLOW	INGRESS	IPv4	SUNND	ubunthosts	any	172.21.95.163/32	any

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

## Relocalisation des agents

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

### Rôles utilisateur

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

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

### Flux de travaux

- Saisissez la clé d'activation, l'adresse IP virtuelle du capteur et l'autorité de certification du capteur (AC), puis [Activer la relocalisation, on page 77](#).
- [Sélectionner les agents à relocaliser, on page 78](#).
- [Désactiver la relocalisation, on page 79](#).



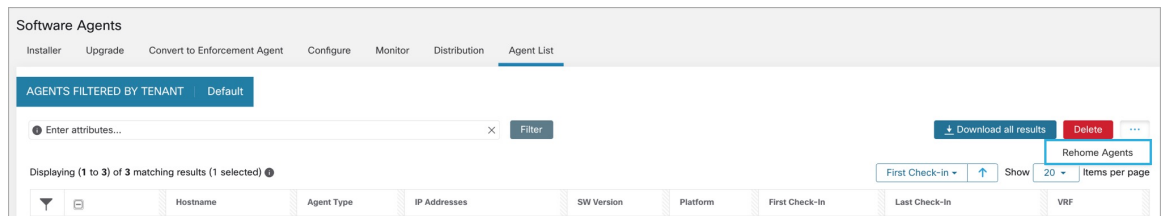
**Note** À tout moment, vous ne pouvez déplacer un agent que vers une seule destination. Nous vous recommandons de désactiver la relocalisation de l'agent après avoir déplacé l'agent.

## Activer la relocalisation

### Procédure

- Étape 1** Dans le volet de navigation, cliquez sur **Manage(Gestion)>Workloads (Charges de travail)> Agents (Agents)**.
- Étape 2** Cliquez sur l'onglet **Agent List** (liste des agents).
- Étape 3** Cliquez sur l'icône de menu et sélectionnez **Rehome Agents** (Relocaliser les agents).

**Figure 16: Agents relocalisés**

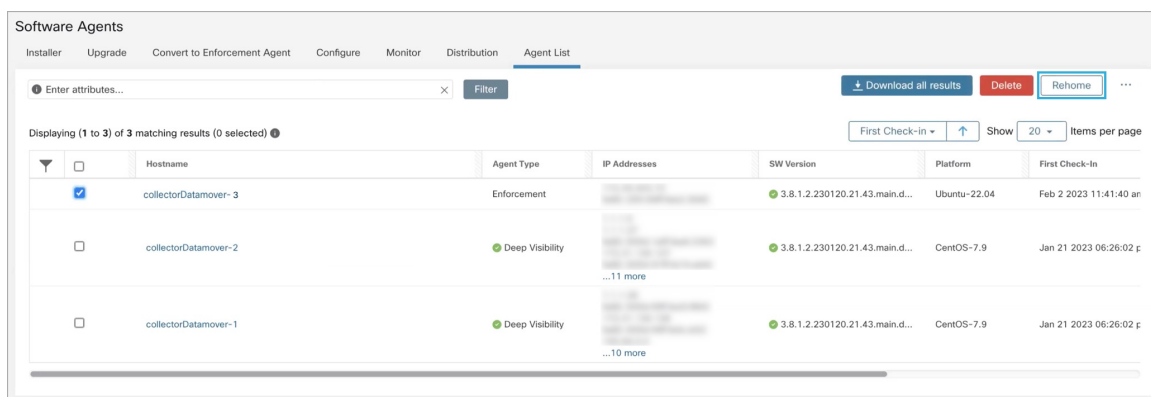


- Étape 4** Dans la fenêtre **Agent Rehomeing**( Relocalisation des agents), saisissez les détails suivants :

Champ	Description
Clé d'activation de la portée de la destination	<ol style="list-style-type: none"> <li>Accédez à <b>Manage (Gestion) &gt; Workloads (Charges de travail) &gt; Agents (Agents)</b>.</li> <li>Cliquez sur l'onglet <b>Installer</b> (Programme d'installation).</li> <li>Sélectionnez <b>Manual install using classic packaged installers (Installation manuelle à l'aide des programmes d'installation classiques)</b>.</li> <li>Cliquez sur <b>Next</b> (suivant).</li> <li>Cliquez sur <b>Agent Activation Key</b> (clé d'activation de l'agent).</li> <li>Copiez la valeur de la <b>clé</b> et collez-la dans le champ <b>Destination Scope Activation Key</b> (Clé d'activation de la portée de destination).</li> </ol>

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

Figure 17: Activer la relocalisation de l'agent



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

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

## Sélectionner les agents à relocaliser

### Procedure

**Étape 1** Sélectionnez un agent.

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

**Figure 18: Sélectionner les agents à relocaliser**

The screenshot shows the 'Software Agents' interface with the 'Agent List' tab selected. At the top, there are navigation tabs: 'Installer', 'Upgrade', 'Convert to Enforcement Agent', 'Configure', 'Monitor', 'Distribution', and 'Agent List'. Below the tabs is a search bar with the text 'Enter attributes...' and a 'Filter' button. To the right of the search bar are buttons for 'Download all results', 'Delete', and 'Rehome' (which is highlighted with a blue border). Below the search bar, it says 'Displaying (1 to 3) of 3 matching results (0 selected)'. There are also controls for 'First Check-in', a refresh icon, 'Show 20', and 'Items per page'. The main area contains a table with columns: Hostname, Agent Type, IP Addresses, SW Version, Platform, and First Check-in. The first row is selected with a blue checkbox and has 'collectorDatamover-3' as the hostname and 'Enforcement' as the agent type. The second and third rows have 'collectorDatamover-2' and 'collectorDatamover-1' as hostnames and 'Deep Visibility' as agent types. Each row has a green status indicator and a 'First Check-in' timestamp.

Host	Agent Type	IP Addresses	SW Version	Platform	First Check-in
collectorDatamover-3	Enforcement	...	3.8.1.2.230120.21.43.main.d...	Ubuntu-22.04	Feb 2 2023 11:41:40 an
collectorDatamover-2	Deep Visibility	...11 more	3.8.1.2.230120.21.43.main.d...	CentOS-7.9	Jan 21 2023 06:26:02 f
collectorDatamover-1	Deep Visibility	...10 more	3.8.1.2.230120.21.43.main.d...	CentOS-7.9	Jan 21 2023 06:26:02 f

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

## Désactiver la relocalisation



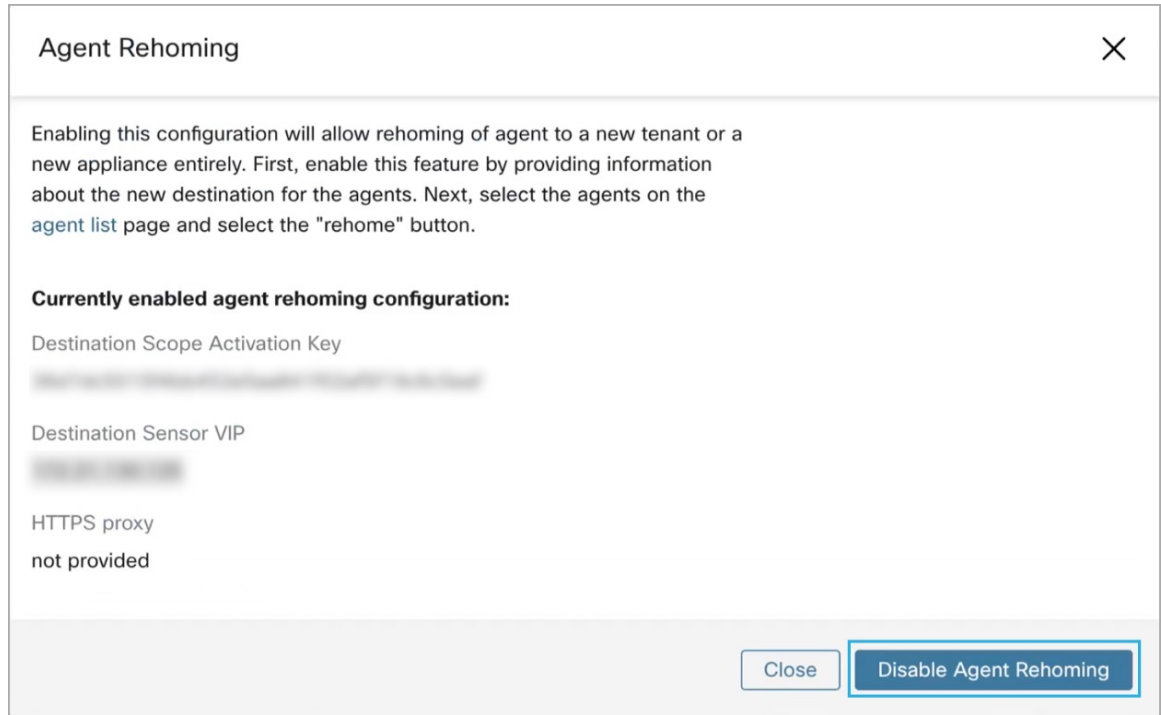
**Note** Si plusieurs utilisateurs se déplacent vers un un logiciel-service SaaS ou à partir de celui-ci, l'administrateur du site doit déplacer chaque détenteur ou appareil séparément. Pour ce faire, désactivez la relocalisation pour effacer les paramètres, puis activez la relocalisation pour le nouvel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

### Procédure

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

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

Figure 19: Désactiver la relocalisation de l'agent



## Générer un jeton d'agent

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

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

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



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

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



## Procédure

---

- Étape 1** Dans le volet de navigation, cliquez sur **Manage (Gestion) > Workloads (Charges de travail) > Agents (Agents) > Agent List (Liste des agents)**.
- Selon vos besoins, vous pouvez choisir l'un des types de jetons d'agent : grappe, détenteur ou propre à l'agent. Pour le jeton propre à l'agent, passez à l'étape 5.
- Étape 2** Cliquez sur l'icône de menu et sélectionnez **Agent Token** (Jeton propre à l'agent).
- Note** L'option de **jeton propre à l'agent** est uniquement visible pour les administrateurs de site ou les rôles d'utilisateur du service d'assistance à la clientèle.
- Étape 3** Sélectionnez un type de jeton
- Token For Cluster (jeton pour la grappe) : Cette option est visible uniquement par les administrateurs de site et le jeton est applicable à tous les agents.
  - Token For Tenant (Jeton pour le détenteur) : applicable pour les agents d'un détenteur sélectionné.
- Étape 4** Pour télécharger la clé de jeton, cliquez sur **Télécharger le jeton**.
- Étape 5** Pour afficher et télécharger les détails de la clé de jeton d'un agent spécifique :
- Allez à l'onglet **Agent List** (Liste des agents) et cliquez sur l'agent requis. Sous **Agent Details (Détails de l'agent) > Agent Token (Jeton de l'agent)**, vous pouvez afficher la clé du jeton et les détails d'expiration du jeton.
  - Pour télécharger le jeton propre à l'agent, cliquez sur **Télécharger le jeton**.
- 

## What to do next

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

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

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

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

### Procédure

---

- Étape 1** Dans l'interface utilisateur Cisco Secure Workload, créez un nouveau profil de configuration d'agent avec la mise en application désactivée.
  - Étape 2** Créez un intent avec la liste des hôtes qui ont besoin d'un changement d'adresse IP avec leur ancienne et leur nouvelle adresse IP.
  - Étape 3** Appliquez le nouveau profil de configuration d'agent à l'intent et enregistrez l'intent.
  - Étape 4** La mise en application doit être désactivée pour ces hôtes sélectionnés.
  - Étape 5** Modifiez l'adresse IP de ces hôtes.
  - Étape 6** Sur l'interface utilisateur Cisco Secure Workload, mettez à jour les filtres de la portée avec la nouvelle adresse IP de ces hôtes.
  - Étape 7** Vérifiez le changement d'adresse IP sous l'onglet Interfaces de la page de profil de charge de travail de l'agent. Dans l'onglet « Politiques » (politiques), assurez-vous que les politiques sont générées avec la nouvelle adresse IP.
  - Étape 8** Supprimez l'intent ou le profil créé ci-dessus.
  - Étape 9** Si la mise en application était désactivée dans le profil de configuration de l'agent d'origine pour la portée, activez-la.
- 

## Mise à niveau des agents logiciels

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

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

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

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

### Procédure

---

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


**Figure 20: Filtre d'inventaire**

+ Create an Inventory Filter


---


1 Define ————— 2 Summary

---

Name  
Development Linux VMs 

Create a query based on Inventory Attributes:  
Inventory is matched dynamically based on the query. The labels can include Hostname, Address/Subnet, OS, and more. The [full list](#) is in the user guide.  
A preview of matching inventory items will be shown in the next step.

Query 

Hostname contains linux 

[Show advanced options](#)

[Cancel](#) [Previous](#) [Next](#)

**Étape 2**

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

Figure 21: Configuration de l'agent

Agent Config Profiles Create Profile

Name ↑	Config	Actions
Default	<p>Enforcement</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Enforcement</li> <li><input checked="" type="checkbox"/> Windows Enforcement Mode - WAF</li> <li><input type="checkbox"/> Preserve Rules</li> <li><input checked="" type="checkbox"/> Allow Broadcast</li> <li><input checked="" type="checkbox"/> Allow Multicast</li> <li><input checked="" type="checkbox"/> Allow Link Local Addresses</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 512MB</li> </ul> <p>Flow Visibility</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Flow Analysis Fidelity - Detailed</li> <li><input checked="" type="checkbox"/> Data Plane</li> <li><input checked="" type="checkbox"/> Auto-Upgrade</li> <li><input type="checkbox"/> PID Lookup</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 512MB</li> </ul> <p>Process Visibility and Forensics</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Forensics</li> <li><input type="checkbox"/> Meltdown Exploit Detection</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 256MB</li> </ul>	<span style="border: 1px solid #007bff; padding: 2px 5px; color: #007bff;">Edit</span> <span style="font-size: 1em;">☰</span>
VM	<p>Enforcement</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Enforcement</li> <li><input checked="" type="checkbox"/> Windows Enforcement Mode - WAF</li> <li><input type="checkbox"/> Preserve Rules</li> <li><input checked="" type="checkbox"/> Allow Broadcast</li> <li><input checked="" type="checkbox"/> Allow Multicast</li> <li><input checked="" type="checkbox"/> Allow Link Local Addresses</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 512MB</li> </ul> <p>Flow Visibility</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Flow Analysis Fidelity - Detailed</li> <li><input checked="" type="checkbox"/> Data Plane</li> <li><input checked="" type="checkbox"/> Auto-Upgrade</li> <li><input type="checkbox"/> PID Lookup</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 512MB</li> </ul> <p>Process Visibility and Forensics</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Forensics</li> <li><input type="checkbox"/> Meltdown Exploit Detection</li> <li><input checked="" type="checkbox"/> CPU Quota Mode - Adjusted (3%)</li> <li><input checked="" type="checkbox"/> Memory Quota Limit - 256MB</li> </ul>	<span style="border: 1px solid #007bff; padding: 2px 5px; color: #007bff;">Edit</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px; margin-left: 10px;">Delete</span> <span style="font-size: 1em;">☰</span>

[View Deleted Agent Config Profiles](#) ☰

**Étape 3**

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

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

Figure 22: Intent de configuration de l'agent

Agent Config Intents

Apply profile  to filter

Apply profile **Default** to filter **Everything**

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

## Mise à niveau manuelle de l'agent

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

### Procédure

- Étape 1** Dans le volet de navigation, cliquez sur **Manage (Gestion) > Workloads (Charges de travail) > Agents (Agents)**.
- Étape 2** Cliquez sur l'onglet **Upgrade** (Mise à niveau). Les agents de visibilité approfondie et d'application sont affichés, et pour chaque agent, seules les versions les plus récentes vers lesquelles l'agent peut être mis à niveau sont répertoriées. Par défaut, la dernière version est sélectionnée.
- Étape 3** Pour filtrer des agents spécifiques, saisissez votre requête de recherche dans la zone de filtre. Par exemple, saisissez Platform = CentOS-7.6.
- Étape 4** Sélectionnez les agents à mettre à niveau à la version sélectionnée et cliquez sur **Upgrade** (Mettre à niveau).

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

## Mettre à niveau le comportement de l'agent Kubernetes/OpenShift

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

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

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

Si la mise à niveau automatique est désactivée pour tous les nœuds, la mise à niveau manuelle est possible en téléchargeant un nouveau script d'installation et en réexécutant l'installation. Le script d'installation détecte automatiquement le cas d'une nouvelle installation par rapport à la mise à niveau d'une installation existante et travaillera pour mettre à niveau manuellement les pods du daemonset lorsqu'il détecte qu'une installation est déjà en place.

## Suppression des agents logiciels

### Supprimer un agent Linux de visibilité approfondie ou d'application

**Installation basée sur le RPM :**

1. Exécutez la commande : **rpm -e tet-sensor**

L'événement de désinstallation de l'agent est communiqué à la grappe et l'agent est marqué comme désinstallé sur la page **Software Agent** (agents logiciels).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (agent logiciel). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.




---

**Note** Par défaut, la **période de nettoyage** est désactivée.

---

**Installation basée sur Ubuntu .deb :**

La nouvelle installation des agents Ubuntu utilise désormais le format natif .deb.

1. Exécutez la commande : **dpkg --purge tet-sensor**

L'événement de désinstallation de l'agent est communiqué à la grappe et l'agent est marqué comme désinstallé sur la page **Software Agent** (agents logiciels).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (agents logiciels). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

**Note**

- Par défaut, la **période de nettoyage** est désactivée.
- Pendant les opérations de l'agent, il est possible que certains modules du noyau soient chargés automatiquement par ce dernier. Par exemple, si l'application est activée sous Linux, les modules Netfilter peuvent être chargés. Les agents n'ont pas de liste des modules chargés par le noyau. Par conséquent, pendant la désinstallation de l'agent, il est impossible de décharger les modules du noyau.
- Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

**Figure 23: Alerte de désinstallation de l'agent**

Hostname	Agent Type	IP Addresses	SW Version	Platform	First Check-in	Last Check-in	VRP
Uninstalled on Feb 9 9:45pm	Enforcement	172.26.231.175 fe80:250:568:fe91:dbdb	3.8.1.2.23013021-enforcer	OracleSolaris-11.4	Feb 9 2023 02:59:20 pm (PST)	Feb 9 2023 08:59:44 pm (PST)	Default
b4-uj-cen0576	Enforcement	172.20.207.106 fe80:4f6c:c6ac:d5e5:a097 192.168.122.1	3.8.1.2.230130.21.43.main.dev-e...	CentOS-7.6	Feb 8 2023 04:38:44 pm (PST)	Feb 8 2023 09:33:26 pm (PST)	Default
sensor-dev-rocky90	Enforcement	10.195.210.122 fe80:250:568:fe91:ca35	3.8.1.2.230130.21.43.main.dev-e...	RockyLinux-9.0	Feb 3 2023 12:02:31 am (PST)	Feb 9 2023 09:01:48 pm (PST)	Default
sensor-dev-oracle9	Enforcement	10.195.210.121 fe80:250:568:fe91:fc2d	3.8.1.2.230130.21.43.main.dev-e...	OracleServer-9.0	Feb 3 2023 12:01:09 am (PST)	Feb 9 2023 09:23:27 pm (PST)	Default
sensor-dev-almal9	Enforcement	10.195.210.120 fe80:250:568:fe91:538b	3.8.1.2.230130.21.43.main.dev-e...	AlmaLinux-9.0	Feb 3 2023 12:00:00 am (PST)	Feb 9 2023 09:22:52 pm (PST)	Default
hartmut-u16	Enforcement	172.26.231.235 fe80:250:568:fe91:34c4	3.7.1.5.devel-enforcer	Ubuntu-16.04	Feb 2 2023 11:27:44 am (PST)	Feb 9 2023 09:19:45 pm (PST)	Default
p91-linux06	Enforcement	172.26.231.235 fe80:250:568:fe91:5902	3.8.1.2.230130.21.43.main.dev-e...	AlmaLinux-9.0	Feb 2 2023 08:48:06 am (PST)	Feb 9 2023 09:20:33 pm (PST)	Default
sensor-dev-deb11	Enforcement	172.20.207.223 fe80:250:568:fe91:a737	3.8.1.2.230130.21.43.main.dev-e...	Debian-11	Feb 2 2023 08:44:43 am (PST)	Feb 9 2023 09:21:10 pm (PST)	Default
agent-req-deb10	Enforcement	10.195.210.132 fe80:250:568:fe91:13d9	3.8.1.2.230130.21.43.main.dev-e...	Debian-10	Feb 2 2023 08:43:18 am (PST)	Feb 9 2023 09:18:56 pm (PST)	Default
sensor-dev-deb9	Enforcement	10.195.210.199 fe80:250:568:fe91:c542	3.8.1.2.230130.21.43.main.dev-e...	Debian-9	Feb 2 2023 08:41:16 am (PST)	Feb 9 2023 09:19:10 pm (PST)	Default
sensor-dev-deb8	Enforcement	10.195.210.145 fe80:250:568:fe91:d8a4	3.8.1.2.230130.21.43.main.dev-e...	Debian-8	Feb 2 2023 08:39:05 am (PST)	Feb 9 2023 09:21:08 pm (PST)	Default
p91-ai09	Enforcement	172.29.157.24 fe80:288a:968:fe09:9202 ac16:9d18	3.8.1.2.230130.21.43.main.dev-e...	AIX-7.2	Feb 1 2023 06:44:31 am (PST)	Feb 9 2023 09:08:44 pm (PST)	Default
collectorDatamover-1	Deep Visibility	1.1.1.26 fe80:5054:acff:fe20:bd3c 10.195.248.22 fe80:5054:acff:fe88:b306 100.54.1.0 10.moss	3.8.1.2.230130.21.43.main.dev-e...	CentOS-7.9	Jan 31 2023 08:08:47 pm (PST)	Feb 9 2023 09:09:39 pm (PST)	Tetration Default

## Suppression d'un agent Windows de visibilité approfondie/de mise en application

Il existe deux options pour désinstaller les agents Cisco Secure Workload :

### Procédure

- Étape 1** Accédez à Panneau de configuration/Programmes/Programmes et fonctionnalités, puis désinstallez **Cisco Secure Workload Agent** (Agent Cisco Tetration).
- Étape 2** Vous pouvez également exécuter le raccourci **Uninstall.lnk** dans « **C:\Program Files\Cisco Tetration** »
- Étape 3** Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

L'événement de désinstallation de l'agent sera communiqué à la grappe et l'agent sera marqué comme désinstallé sur la page **Software Agent** (Agent logiciel).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (Agent logiciel). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

**Note** Par défaut, la **période de nettoyage** est désactivée.

**Note**

- Si Npcap a été installé lors de l'installation de l'agent, il sera également désinstallé.
- Par défaut, les fichiers journaux, les fichiers de configuration et les certificats ne seront pas supprimés lors de la désinstallation. Si vous souhaitez les supprimer, exécutez le raccourci **UninstallAll.lnk** dans le même dossier.

---

## Supprimer un agent AIX de visibilité approfondie ou d'application

### Procédure

---

Exécutez la commande : « **installp -u tet-sensor** ».

L'événement de désinstallation de l'agent sera communiqué à la grappe et l'agent sera marqué comme désinstallé sur la page **Software Agent** (Agent logiciel).

Supprimez manuellement l'agent de l'interface utilisateur sur la page **Software Agent** (Agent logiciel). Sinon, l'utilisateur peut activer le nettoyage automatisé ou la suppression de l'agent en activant la **période de nettoyage** à partir des profils de configuration d'agent.

**Note**

- Par défaut, la **période de nettoyage** est désactivée.
- L'agent de visibilité approfondie est contrôlé par le contrôleur de ressources système en tant que tet-sensor. Il est possible de le démarrer, l'arrêter, le redémarrer et le supprimer. Le service est rendu persistant avec inittab en tant que tet-sen-engine.
- L'agent d'application est contrôlé par le contrôleur de ressources système en tant que tet-enforcer. Il est possible de le démarrer, l'arrêter, le redémarrer et le supprimer. Le service est rendu persistant avec inittab en tant que tet-enf-engine.
- Pendant les opérations de l'agent, il est possible que certains modules du noyau soient chargés automatiquement par ce dernier. Par exemple, si l'application est activée dans AIX, les modules ipfilter sont chargés. Les agents n'ont pas de liste des modules chargés par le noyau. Par conséquent, pendant la désinstallation de l'agent, il est impossible de décharger les modules du noyau.
- Si l'agent d'application a appliqué une politique au pare-feu du système, la désinstallation de l'agent efface la politique appliquée et ouvre le pare-feu du système.

---



## Supprimer l'agent Universal Linux

### Procédure

---

- Étape 1** Exécutez le script de désinstallation : « `/usr/local/tet-light/uninstall.sh` »
- Étape 2** Supprimez l'agent de l'interface utilisateur dans la page **Software Agent (agent logiciel)**.
- 

## Supprimer l'agent Windows universel

### Procédure

---

- Étape 1** Exécutez le script de désinstallation : « `C:\Program Files\Cisco Tetration\Lightweight Sensor\uninstall.cmd` »
- Étape 2** Supprimez l'agent de l'interface utilisateur dans la page **Software Agent (agent logiciel)**.
- 

## Supprimer un agent d'application Kubernetes ou OpenShift

### Procédure

---

- Étape 1** Localisez le script du programme d'installation d'origine ou téléchargez un nouveau script à partir de l'interface utilisateur Cisco Secure Workload.
- Étape 2** Exécutez l'option de désinstallation : `install.sh --uninstall`. Les mêmes considérations s'appliquent que lors de l'installation.
- Pris en charge uniquement sur les architectures Linux x86\_64.
  - `~/kube/config` contient un utilisateur d'informations d'authentification d'administrateur ou utilisez l'option `--kubeconfig` pour pointer vers le fichier d'informations d'authentification de l'administrateur `kubectl`.
- Étape 3** Supprimez les agents pour tous les nœuds Kubernetes de l'interface utilisateur sur la page **Software Agent (Agents logiciels)**
- 

## Supprimer un agent de visibilité approfondie Solaris

### Procédure

---

- Étape 1** Exécutez la commande : `pkg uninstall tet-sensor`

**Étape 2** Supprimez l'agent dans la page **Software Agent** (Agent logiciel).

---

## Données collectées et exportées par les agents de charge de travail

Cette section décrit les principaux composants d'un agent logiciel, la façon dont il est enregistré auprès des services dorsaux (backend) et les données qui sont collectées et exportées vers la grappe à des fins d'analyse.

### Inscription

Une fois que l'agent a été installé avec succès sur le système, il doit s'inscrire auprès des services dorsaux pour obtenir un identifiant unique valide. Les renseignements suivants sont envoyés avec la demande d'enregistrement :

- Nom d'hôte
- BIOS-UUID
- Informations sur la plateforme (telle que CentOS-6.5)
- Certificat client généré automatiquement (généré avec la commande openssl)
- Type d'agent (visibilité ou application)

Si l'agent ne parvient pas à obtenir un ID valide du serveur, il réessaiera jusqu'à ce qu'il en obtienne. Il est très important que l'agent soit enregistré, sinon toutes les communications ultérieures avec d'autres services (comme les collecteurs) seront rejetées.

### Mise à niveau de l'agent

Périodiquement (environ toutes les 30 minutes), l'agent envoie un message au service de serveur principal (backend) pour signaler sa version actuelle. Le service de serveur principal utilise l'ID de l'agent et sa version actuelle pour décider si un nouveau paquet est disponible pour l'agent. Les renseignements suivants sont envoyés :

- ID de l'agent (obtenu après un enregistrement réussi)
- Version actuelle de l'agent

### Serveur de configuration

Les agents exportent les informations suivantes vers le serveur de configuration configuré :

- Nom d'hôte
- ID de l'agent (obtenu après un enregistrement réussi)
- Liste des interfaces, chacune d'entre elles comprend
  1. Nom de l'interface

2. Famille IP (IPv4 ou IPv6)
3. Adresses IP
4. Masque réseau
5. Adresses MAC
6. Indice d'interface

Dès que une propriété d'interface change (comme l'adresse IP d'une interface existante change, ou une nouvelle interface apparaît), cette liste est actualisée et signalée au serveur de configuration.

## Network flow

Network Flow information is the summarization of all packets flowing through the system. There are two modes of capturing flow information: Detailed and Conversation. By default the Detailed mode of capture is used. The captured flows are exported to collector, the exported information includes:

- Flow identifier: uniquely identify the network flow. It includes the general information such as: IP protocol, source and destination IP, and layer 4 ports
- IP Information: contains information seen in IP header, such as: TTL, IP flags, Packet ID, IP options and Fragmentation flags
- TCP Information: contains information seen in TCP header, such as: sequence number, Ack number, TCP options, Rcvd windows size
- Flow Information: flow's statistics (such as: total packets, total bytes, TCP flags statistics, packet length statistics and socket statistics), interface index from which flow was observed, flow's start time and end time

In Conversation mode, agents will only export TCP flows that are bi-directional in nature along with other connectionless flows. Conversation mode is supported for Windows, AIX and Linux platforms. For more information on Conversation mode, see [Conversation Mode](#).



---

**Note** In K8s environment, correlation of Pod/Host flows will not be done in Conversation mode.

---

Note that in either mode agent will not export the following flows:

- ARP/RARP conversations
- Agent's flows to collectors

## Renseignements sur la machine

Les renseignements sur la machine décrivent tous les processus en cours d'exécution sur l'hôte. En outre, ils contiennent des informations sur le réseau associées aux processus et sur la commande utilisée pour lancer les processus. Les renseignements sur la machine sont exportés toutes les minutes et comprennent les éléments suivants :

- Identifiant de processus
- Identifiant de l'utilisateur : propriétaire du processus

- ID du processus parent
- Chaîne de commande utilisée pour lancer le processus
- Renseignements sur le socket : protocole (comme UDP ou TCP), type d'adresse : IPv4 ou IPv6, adresse IP source et de destination, ports source et de destination, état TCP, heures de début et de fin du processus, chemin d'accès au fichier binaire
- Renseignements criminalistiques : pour en savoir plus, consultez la section [Compatibilité](#).

## Statistiques des agents

L'agent effectue le suivi de diverses statistiques, y compris les statistiques du système et les siennes, notamment :

- Heure de début et durée de disponibilité de l'agent
- Durée d'exécution de l'agent en mode utilisateur et en mode noyau
- Le nombre de paquets reçus et abandonnés
- Nombre de connexions SSL réussies et échouées
- Flux total de paquets et d'octets
- Total des flux et paquets exportés vers les collecteurs
- Utilisation de la mémoire et de la CPU de l'agent

## Alertes de mise en application

Il existe trois types d'alertes de mise en application :

- Accessibilité de l'agent

Cette alerte détecte lorsque l'agent n'est pas accessible. Cette alerte se déclenche si l'agent n'a pas communiqué avec la grappe Cisco Secure Workload pendant une durée supérieure au nombre de secondes configuré.

### Configure Enforcement Alerts

Configured Alerts

- Scope: **Tetration** when **Agent not reachable (seconds) > 300**
- Scope: **Tetration** when **Firewall = Off**
- Scope: **Tetration** when **Policy = Deviated**

[More details ...](#)

Types

Agent Reachability ⓘ  Workload Firewall ⓘ  Workload Policy ⓘ

For Scope: **Tetration**

Agent not reachable (seconds) > 3000 ⓘ

Severity

Low  Medium  High  Critical  Immediate Action

Hide Advanced Settings ^

Individual Alerts

Enable  Disable

Summary Alerts

None  Hourly  Daily

- Pare-feu de charge de travail

Cette alerte se déclenche si l'application est configurée sur un charge de travail mais que le pare-feu est détecté comme désactivé, car cette condition empêchera l'agent Cisco Secure Workload d'appliquer les politiques de trafic.

Configure Enforcement Alerts
✕

---

Configured Alerts

- Scope: **Tetration** when **Agent not reachable (seconds) > 300**
- Scope: **Tetration** when **Firewall = Off**
- Scope: **Tetration** when **Policy = Deviated**

[More details ...](#)

---

Types

Agent Reachability ⓘ
Workload Firewall ⓘ
Workload Policy ⓘ

For Scope: **Tetration**

■ **Firewall is Off** ✕

Severity

Low
Medium
High
Critical
Immediate Action

Hide Advanced Settings ^

Individual Alerts

Enable
Disable

Summary Alerts

None
Hourly
Daily

Dismiss
Create

- Politique de charge de travail

Cette alerte se déclenche si les règles du pare-feu de charge de travail sont différentes des politiques Cisco Secure Workload applicables à cette charge de travail (les « politiques concrètes » de la charge de travail)

Configure Enforcement Alerts
✕

---

Configured Alerts

- 🗑 Scope: **Tetration** when **Agent not reachable (seconds) > 300**
- 🗑 Scope: **Tetration** when **Firewall = Off**
- 🗑 Scope: **Tetration** when **Policy = Deviated**

[More details ...](#)

---

Types

Agent Reachability ⓘ
Workload Firewall ⓘ
Workload Policy ⓘ

For Scope: **Tetration**

ⓘ **Policy is Deviated** ✕

Severity

Low
Medium
High
Critical
Immediate Action

---

Hide Advanced Settings ^

Individual Alerts

Enable
Disable

Summary Alerts

None
Hourly
Daily

Dismiss
Create

Figure 24: Types d'alertes de mise en application

Configure Enforcement Alerts See All Configured Enforcement Alerts ×

Alert Name ⓘ  
Agent\_Not\_Reachable

Alert Types ⓘ  
**Agent Reachability** Workload Firewall Workload Policy

For Scope: **TenantTesting**

Alert Condition ⓘ  
Agent not Reachable (seconds) > 300 ×

Severity  
**Low** **Medium** High Critical Immediate Action

Hide Advanced Settings ^

Individual Alerts  
**Enable** Disable

Summary Alerts  
**None** Hourly Daily

Cancel Save

Vous pouvez définir la gravité de l'alerte ainsi que d'autres paramètres de configuration par type. Pour configurer les alertes de mise application, consultez [Configurer les alertes](#).



Figure 25: Configuration des alertes de mise en application

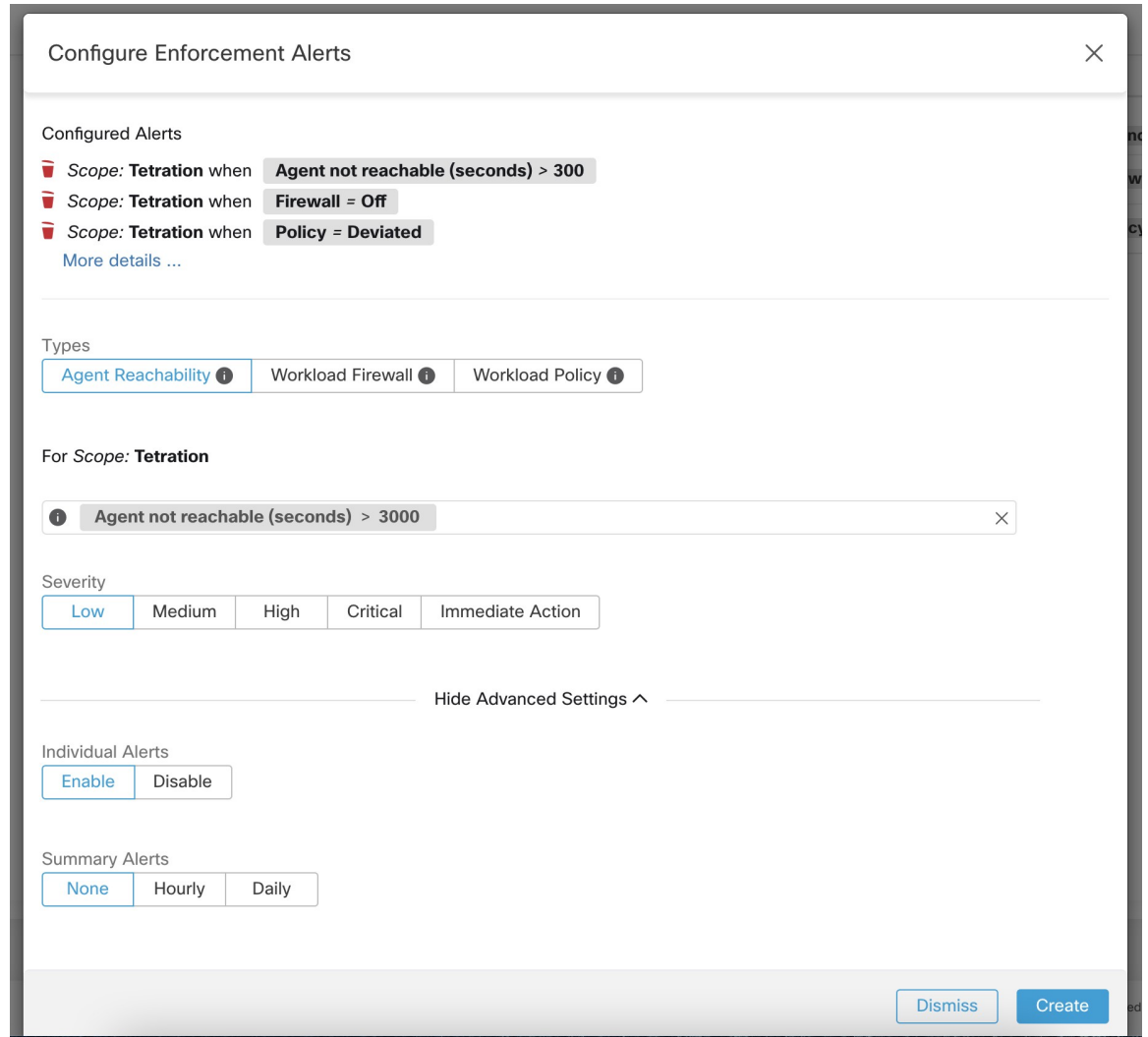
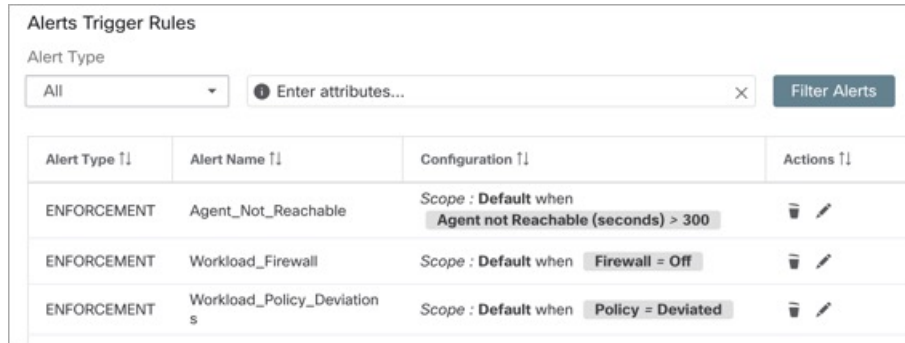


Figure 26: Affichage des alertes de mise en application configurées sur la page de configuration des alertes

### Alerts Trigger Rules

Alert Type ↑↓	Configuration ↑↓	Actions ↓
ENFORCEMENT	Scope: <b>Tetration</b> when <b>Agent not reachable (seconds) &gt; 300</b>	
ENFORCEMENT	Scope: <b>Tetration</b> when <b>Firewall = Off</b>	
ENFORCEMENT	Scope: <b>Tetration</b> when <b>Policy = Deviated</b>	

Figure 27: Afficher les alertes de mise en application configurées



## Détails des alertes de l'interface utilisateur d'application

Figure 28: Détails de l'alerte d'application

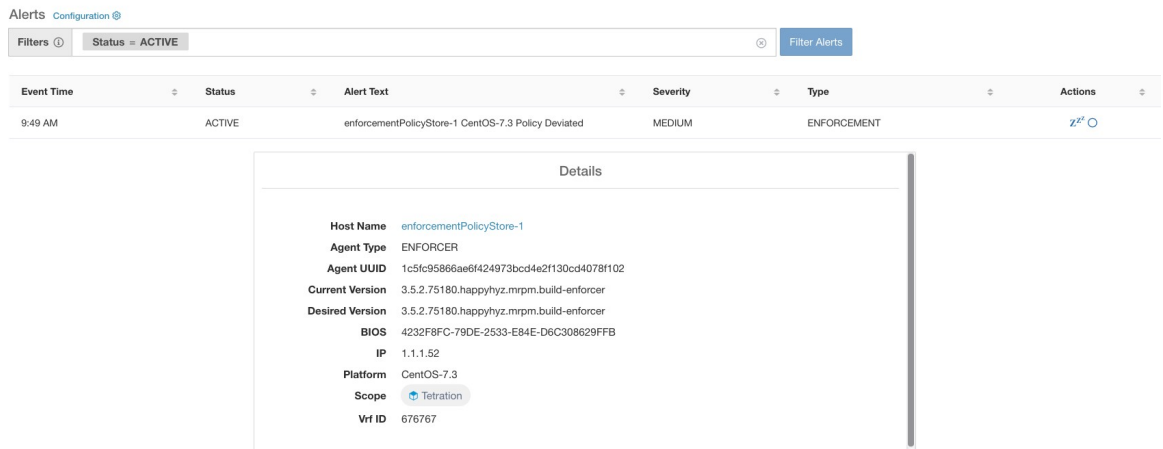
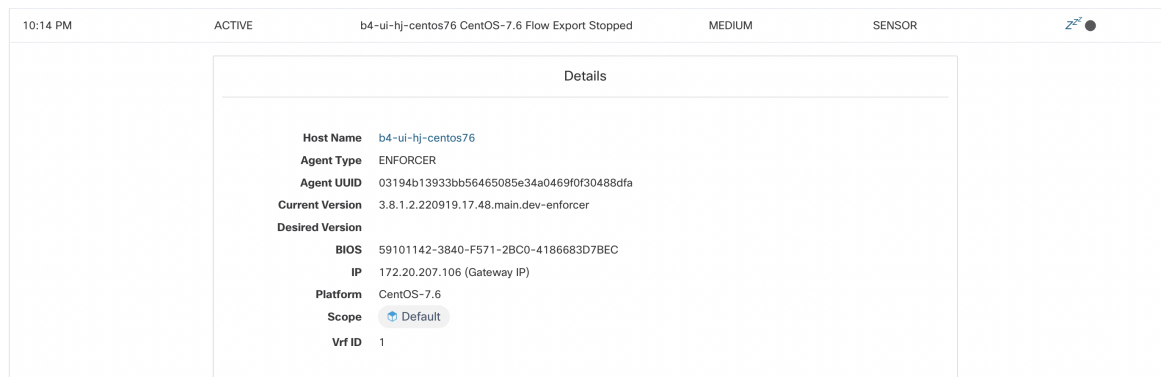


Figure 29: Détails d'alertes d'application lorsque le serveur mandataire est activé sur l'hôte



## Détails de l'alerte d'application

Consultez [Common Alert Structure \(Structure d'alerte commune\)](#) pour obtenir la structure générale des alertes et des informations sur les champs. Le champ `alert_détails` est structuré et contient les sous-champs suivants pour les alertes de mise en application

Champ	Type d'alerte	Format	Explication
Type d'agent	<i>tous</i>	chaîne	« ENFORCER » (APPLICATEUR) ou « SENSOR » (CAPTEUR) selon le type d'installation
Nom de l'hôte :	<i>tous</i>	chaîne	Nom de l'hôte sur lequel l'agent est déployé
IP	<i>tous</i>	chaîne	Adresse IP du nœud ou de la passerelle
Biographies	<i>tous</i>	chaîne	UUID BIOS du nœud
Observations	<i>tous</i>	chaîne	Renseignements sur la plateforme ou le système d'exploitation du nœud
Version actuelle	<i>tous</i>	chaîne	Version du logiciel de l'agent sur le nœud
Version souhaitée	<i>tous</i>	chaîne	Version du logiciel souhaitée pour l'agent
LastConfigFetchAt	<i>tous</i>	nombre entier	Horodatage Unix de la dernière fois que l'agent a envoyé une requête https

### Exemple de détails\_alertes pour une alerte de mise en application

```
{
  "AgentType": "ENFORCER",
  "Bios": "72EF1142-03A2-03BC-C2F8-F600567BA320",
  "CurrentVersion": "3.5.1.1.mrpm.build.win64-enforcer",
  "DesiredVersion": "",
  "HostName": "win2k12-production-db",
  "IP": "172.26.231.193",
  "Platform": "MSServer2012R2Standard"
}
```

## Alertes de capteurs

La configuration des alertes de capteur permet de configurer différents types d'alertes. Vous pouvez définir la gravité de l'alerte et les types de paramètres de configuration.

Pour en savoir plus, consultez [Boîte de dialogue modale de configuration des alertes](#).



**Note** À partir de Cisco Secure Workload 3.5, vous pouvez configurer les alertes de capteur à l'aide du *modèle d'alerte de configuration*.

**Figure 30: Configurer les alertes de capteur**

**Configure Sensors Alerts** [X]

Configured Alerts

- Scope: Default when Agent Upgrade Status = Failed
- Scope: Default when Agent Flow Export Status = Stopped
- Scope: Default when Agent Check-In Service = Inactive

[More details ...](#)

**Types** Agent Upgrade ⓘ Agent Flow Export ⓘ Agent Check In ⓘ

For Scope: Default

**When** ⓘ Agent Upgrade Status is Failed ⓘ

**Severity** Low Medium High Critical Immediate Action

Hide Advanced Settings ^

**Individual Alerts** Enable Disable

**Summary Alerts** None Hourly Daily

Create Dismiss

**Configure Sensors Alerts** [X]

Configured Alerts

- Scope: Default when Agent Upgrade Status = Failed
- Scope: Default when Agent Flow Export Status = Stopped
- Scope: Default when Agent Check-In Service = Inactive

[More details ...](#)

**Types** Agent Upgrade ⓘ Agent Flow Export ⓘ Agent Check In ⓘ

For Scope: Default

**When** ⓘ Agent Upgrade Status is Failed ⓘ

**Severity** Low Medium High Critical Immediate Action

Hide Advanced Settings ^

**Individual Alerts** Enable Disable

**Summary Alerts** None Hourly Daily

**Create** **Dismiss**

Configurer les alertes du capteur pour signaler l'échec de la mise à niveau d'un agent. Cette alerte se déclenche si l'agent n'a pas réussi à effectuer la mise à niveau vers la version nécessaire.

**Configure Sensors Alerts** [X]

Configured Alerts

- Scope: **Default** when **Agent Upgrade Status = Failed**
- Scope: **Default** when **Agent Flow Export Status = Stopped**
- Scope: **Default** when **Agent Check-In Service = Inactive**

[More details ...](#)

**Types** Agent Upgrade ⓘ Agent Flow Export ⓘ Agent Check In ⓘ

For Scope: **Default**

**When** ⓘ Agent Flow Export Status is Stopped ⓘ

**Severity** Low Medium High Critical Immediate Action

Hide Advanced Settings ^

**Individual Alerts** Enable Disable

**Summary Alerts** None Hourly Daily

Create Dismiss

Configurer les alertes du capteur pour détecter quand l'exportation de flux d'agent doit s'arrêter. Cette alerte se déclenche si la connectivité est bloquée entre l'agent et la grappe, empêchant ainsi les flux et autres informations système d'être envoyées ou fournies.

**Configure Sensors Alerts** [X]

Configured Alerts

- Scope: Default when Agent Upgrade Status = Failed
- Scope: Default when Agent Flow Export Status = Stopped
- Scope: Default when Agent Check-In Service = Inactive

[More details ...](#)

**Types** Agent Upgrade ⓘ Agent Flow Export ⓘ **Agent Check In ⓘ**

For Scope: Default

**When ⓘ** Agent Check-In Service is Inactive ⓘ

**Severity** **Low** Medium High Critical Immediate Action

Hide Advanced Settings ^

**Individual Alerts** **Enable** Disable

**Summary Alerts** **None** Hourly Daily

**Create** Dismiss

Configurer les alertes des capteurs pour détecter l'expiration du délai de vérification de l'agent. Cette alerte se déclenche si la grappe ne reçoit pas de demande d'enregistrement d'un agent pendant plus de 90 minutes.

Figure 31: Configurer les alertes de capteur

Configure Sensors Alerts
See All Configured Sensors Alerts ✕

Alert Name ?

Alert Types ?

Agent Upgrade

Agent Flow Export

Agent Check In

Agent Memory Usage

Agent CPU Quota

Amount Of Flow Observations

New Agent Registered

Pcap Status

Agent Uninstalled

Not Recommended Cipher

Deprecated TLS Version

Agent Auto Removal

For Scope: **Default**

Alert Condition ?

Severity

Low

Medium

High

Critical

Immediate Action

Hide Advanced Settings ^

Individual Alerts

Enable

Disable

Summary Alerts

None

Hourly

Daily

Cancel Create

Figure 32: Configurer les alertes de capteur dans la configuration des alertes

Alerts Trigger Rules

Filters ? Alert type = sensors Filter Alerts

Alert Type	Configuration	Actions
SENSORS	Scope: Default when <span style="background-color: #f0f0f0; padding: 2px;">Agent Upgrade Status = Failed</span>	<span>✕</span>
SENSORS	Scope: Default when <span style="background-color: #f0f0f0; padding: 2px;">Agent Flow Export Status = Stopped</span>	<span>✕</span>
SENSORS	Scope: Default when <span style="background-color: #f0f0f0; padding: 2px;">Agent Check-In Service = Inactive</span>	<span>✕</span>



Figure 33: Afficher les alertes de capteur

Alerts Trigger Rules

Alert Type: SENSORS

Alert Type	Alert Name	Configuration	Actions
SENSORS	Upgrade_Status	Scope : Tetration when Agent Upgrade Status = Failed	
SENSORS	Iface_Flow_Export_Status	Scope : Tetration when Agent Flow Export Status = Stopped	
SENSORS	Upgrade_Srv_CheckIn	Scope : Tetration when Agent Check-In Service = Inactive	
SENSORS	Agent_Mem_Usage	Scope : Tetration when Deep Visibility Memory Usage (MB) > 512 and Enforcement Memory Usage (MB) > 512 and Forensic Memory Usage (MB) > 256	
SENSORS	Agent_CPU_Quota	Scope : Tetration when Deep Visibility CPU Quota (%) > 3 and Enforcement CPU Quota (%) > 3 and Forensic CPU Quota (%) > 3	
SENSORS	Amt_Of_Flow_Obs	Scope : Tetration when Amount of Flow Observations > 500000	
SENSORS	Agent_Uninstalled	Scope : Tetration when Agent Uninstalled = On	
SENSORS	Agent_Auto_Removal	Scope : Tetration when Alert before Removal (minutes) = 5	

## Détails des alertes de l'interface utilisateur des capteurs

Figure 34: Alertes de capteurs

Alerts Configuration

Filters: Status = ACTIVE

Event Time	Status	Alert Text	Severity	Type	Actions
11:13 AM	ACTIVE	b4-ui-centos76 CentOS-7.6 Agent Inactive	MEDIUM	SENSOR	

Details

Host Name: b4-ui-centos76

Agent Type: ENFORCER

Agent UUID: c6c2fbed5e510f5f4eb43b98d30add8ab3fd907

Current Version: 3.6.1.2.201213.21.41.main.dev-enforcer

Desired Version:

BIOS: 59101142-3840-F571-2BC0-4186683D7BEC

IP: 172.20.207.106

Platform: CentOS-7.6

Scope:

Vrf ID: 1

## Détails de l'alerte de capteur

Pour connaître la structure générale des alertes et pour en savoir plus sur les champs, consultez la section Structure commune des alertes. Le champ *alert\_details* (détails des alertes) est structuré et contient les sous-champs suivants pour les alertes de capteurs

## Exemple de détails\_alertes pour une alerte de capteur

Champ	Type d'alerte	Format	Explication
Type d'agent	<i>tous</i>	chaîne	« ENFORCER » (APPLICATEUR) ou « SENSOR » (CAPTEUR) selon le type d'installation
Nom de l'hôte :	<i>tous</i>	chaîne	Nom de l'hôte sur lequel l'agent est déployé
IP	<i>tous</i>	chaîne	Adresse IP du nœud ou de la passerelle
Biographies	<i>tous</i>	chaîne	UUID BIOS du nœud
Observations	<i>tous</i>	chaîne	Renseignements sur la plateforme ou le système d'exploitation du nœud
Version actuelle	<i>tous</i>	chaîne	Version du logiciel de l'agent sur le nœud
Version souhaitée	<i>tous</i>	chaîne	Version du logiciel souhaitée pour l'agent
LastConfigFetchAt	<i>tous</i>	nombre entier	Horodatage Unix de la dernière fois que l'agent a envoyé une requête HTTPS

## Exemple de détails\_alertes pour une alerte de capteur

```
{
  "AgentType": "SENSOR",
  "Bios": "72EF1142-03A2-03BC-C2F8-F600567BA320",
  "CurrentVersion": "3.5.1.1.mrpm.build.win64-sensor",
  "DesiredVersion": "",
  "HostName": "win2k12-production-db",
  "IP": "172.26.231.193",
  "Platform": "MSServer2012R2Standard"
}
```

## 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.