Surveiller les configurations dans Cisco Secure Workload

Les options de **surveillance** qui s'offrent à vous varient en fonction de votre rôle.

- Surveillance des agents, on page 1
- Type de surveillance des agents, on page 1
- État et statistiques de l'agent, on page 3
- État d'application, on page 5
- État d'application pour les connecteurs infonuagiques, on page 6
- Suspendre les mises à jour des politiques, on page 7

Surveillance des agents

La page affiche le nombre de tous les agents surveillés dans une grappe en fonction de la portée racine actuellement sélectionnée.

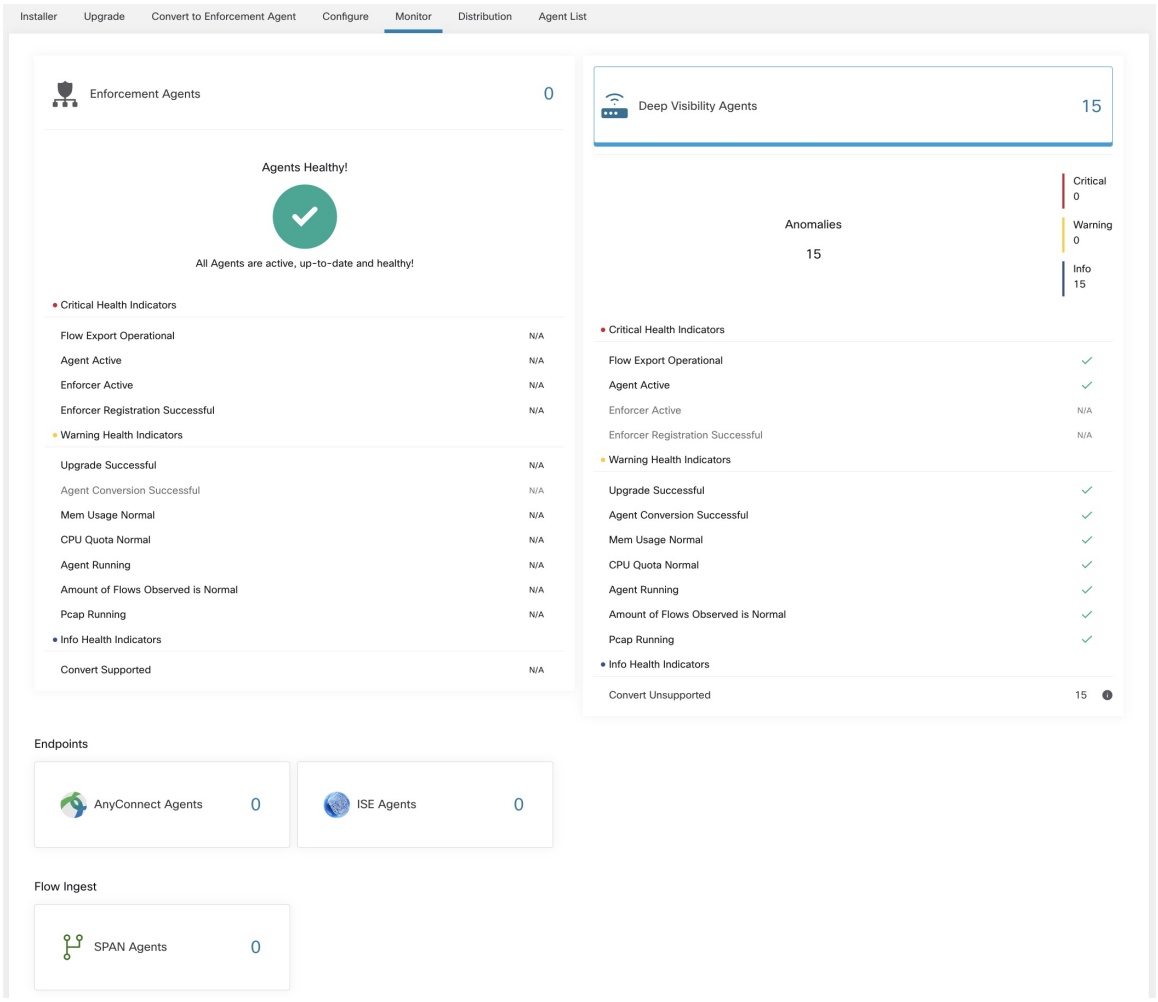
Note Le décompte total des inventaires correspond à la somme de tous les inventaires observés sur le réseau après l'application des règles de collecte.

Type de surveillance des agents

Pour surveiller les agents, cliquez sur **Manage (Gestion)** > **Agents (Agents)** dans la barre de navigation de gauche, puis cliquez sur l'onglet **Monitor** (Surveiller).

Cette page est uniquement disponible pour les utilisateurs qui ont les rôles d' **administrateur du site** et de **service d'assistance à la clientèle**. Les **propriétaires de portée** peuvent voir l'inventaire, les agents de visibilité approfondie et les agents d'exécution.

Figure 1: Nombre total d'agents installés



Le tableau suivant présente les différences entre chaque type d'agent.

Type d'agent	Description
Visibilité accrue	Fournit la précision la plus élevée en termes de séries temporelles de données de flux, de processus s'exécutant sur un hôte. La plupart des plateformes Linux et Windows sont prises en charge. See sw_agents_deployment-label
Exécution	Fournit toutes les fonctionnalités disponibles pour les agents de visibilité approfondie. En outre, les agents de mise en application peuvent définir des règles de pare-feu sur l'hôte installé.

AnyConnect	Fournit des données de flux de séries chronologiques sur les points terminaux exécutant l'agent de mobilité sécurisée AnyConnect avec module de visibilité réseau (NVM) sans nécessiter l'installation d'un agent Cisco Cisco Secure Workload. Les enregistrements IPFIX générés par NVM sont envoyés au connecteur serveur mandataire Cisco Secure Workload AnyConnect. Windows, Mac et certaines plateformes de téléphone intelligent sont prises en charge.
ISE	Fournit les métadonnées des points terminaux enregistrés auprès de Cisco ISE. Grâce à ISE pxGrid, le connecteur ISE collecte les métadonnées, enregistre les points terminaux ISE sur Cisco Secure Workload pendant que les agents ISE envoient des étiquettes en fonction des attributs extraits de l'appareil ISE et des attributs LDAP pour les utilisateurs connectés aux points terminaux.
Le tableau suivant présente un bref résumé des divers agents d'appareils fournis par Cisco Cisco Secure Workload.	
Agents d'appareil	Description
SPAN	Fournit l'analyse du flux sans nécessiter d'installation d'agent par hôte. Il s'exécute sur l'appareil de machine virtuelle Cisco Secure Workload ERSPAN. Il consomme des paquets ERSPAN provenant de n'importe quel commutateur Cisco.

Note Les agents d'appareil tels que NetFlow, NetScaler, F5, AWS et AnyConnect Proxy sont désormais pris en charge en tant que connecteurs. Pour plus d'informations sur les connecteurs, consultez Que sont les connecteurs.

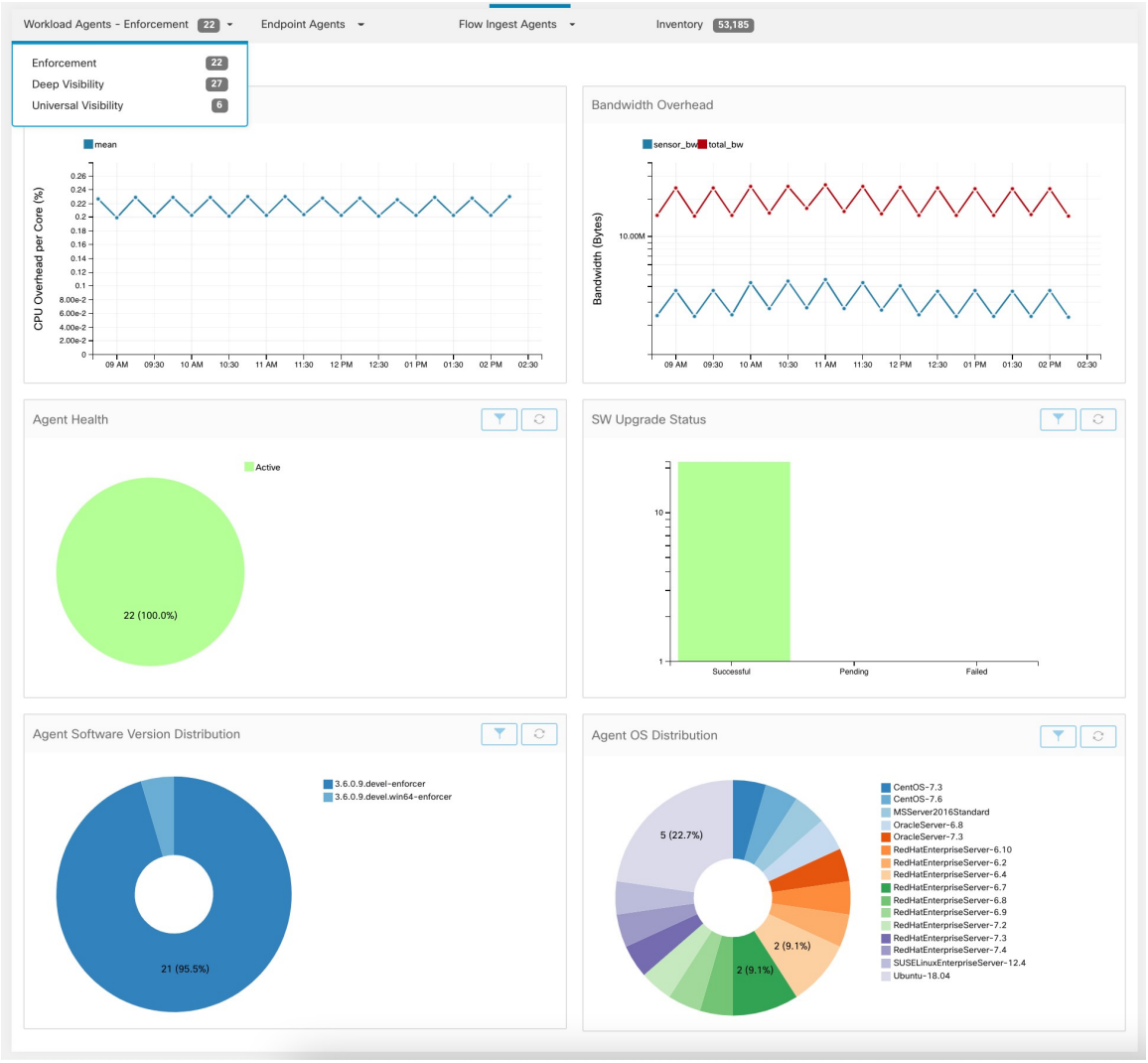
Tout bouton de type d'agent différent de zéro permet d'approfondir la répartition de chaque type d'agent.

État et statistiques de l'agent

Pour afficher les tableaux décrits dans cette rubrique, choisissez **Manage (Gestion) > Agents (Agents)**, puis cliquez sur l'onglet **Distribution (Répartition)**.

Les tableaux suivants sont disponibles pour les types d'agents de visibilité approfondie et d'application.

Figure 2: Répartition des Agents



Pour chaque type d'agent, cette page fournit un aperçu et l'intégrité des agents enregistrés, y compris la surcharge globale du processeur, la surcharge de la bande passante, les paquets manqués, la distribution du système d'exploitation/dans la version et l'état de la mise à niveau de l'agent.

Tableau de surcharge du processeur

Le tableau CPU Overhead (Surcharge du processeur) fournit une vue agrégée de la surcharge de CPU par cœur pour tous les agents. La surcharge de CPU par agent est fournie dans le cadre du profil de charge de travail. Ce tableau n'est disponible que pour les types d'agents de visibilité approfondie et d'application.

Tableau de surcharge de la bande passante

Le tableau Bandwidth Overhead (Surcharge de la bande passante) fournit des statistiques agrégées sur la bande passante totale et la bande passante utilisée par les agents. La surcharge de bande passante par agent est fournie dans le profil de charge de travail. Ce tableau n'est disponible que pour les types d'agents de visibilité approfondie et d'application.

Tableau de l'intégrité des agents

Le tableau Agent Health (Intégrité de l'agent) fournit le nombre d'agents actifs ou inactifs. Les agents actifs sont ceux qui communiquent avec le serveur de configuration pour les mises à niveau à des intervalles réguliers. L'intervalle de vérification est de 30 minutes. Si nous pouvons constater qu'un agent a manqué plus de deux périodes de vérification d'agent, il sera déclaré inactif.

Tableau des mises à jour des agents logiciels vers les dernières révisions

Chaque fois qu'un agent se connecte au serveur de configuration, l'agent fournit également sa version actuelle de RPM. Si un agent est configuré avec une version précise et n'est pas en mesure d'effectuer la mise à jour après deux périodes de vérification, l'agent sera déclaré impossible à mettre à niveau à la dernière version.

Tableau des paquets manqués par l'agent

Dans de rares cas, lorsque le volume de trafic traversant un hôte est supérieur au taux d'inspection de l'agent, certains paquets ne sont pas analysés. Le nombre de paquets manqués et le nom de l'agent correspondant sont affichés dans ce tableau.

Tableaux de répartition des versions du logiciel et du système d'exploitation de l'agent

Ces tableaux montrent la répartition des versions de l'agent et de la plateforme de système d'exploitation parente de tous les agents enregistrés auprès de la grappe Cisco Secure Workload.

État d'application

Pour afficher l'état d'application, cliquez sur **Defend (Défendre)** > **Enforcement Status (État d'application)** dans la barre de navigation à gauche de la fenêtre.

Cette page est accessible pour les administrateurs de site, les utilisateurs du service d'assistance à la clientèle et les propriétaires de portée qui souhaitent obtenir un aperçu de l'état actuel de tous les agents d'application, y compris les connecteurs infonuagiques qui appliquent une politique.

Si l'un des tableaux est rouge ou orangé, consultez la rubrique applicable :

Table 1: Tableaux de l'état d'application

Tableau	Résultat	Passer à l'action
Application par les agents activée	**Désactivée**	Vérifiez que l'application est activée dans la configuration de l'agent. Consultez Créer un profil de configuration d'agent.
Configuration de politique de l'agent	**politiques périmées**	Cette situation est généralement temporaire et ne nécessite généralement aucune action. Cela se produit car un déploiement Cisco Secure Workload basé sur des étiquettes met à jour l'inventaire et les politiques de manière dynamique. Toutefois, si la situation persiste pour certaines charges de travail individuelles, communiquez avec Cisco TAC.
Politiques concrètes des agents	**Sauté**	Cela indique que les politiques n'ont pas été envoyées à certains agents.

Tip

- Pour afficher l'état de portées individuelles ou pour l'ensemble du détenteur, utilisez l'option **Filter by Scope** (filtrer par portée) dans le côté supérieur gauche de la page.
- Si les tableaux indiquent un problème, identifiez les charges de travail concernées en cliquant dans la partie correspondante du tableau.

  Le tableau affiche les charges de travail concernées.

  Pour voir les options de filtrage, vous pouvez également cliquer sur le bouton (i) dans la zone **Filter** (Filtrer) sous les tableaux.
- Pour afficher un grand nombre de détails supplémentaires, cliquez sur le lien IP address (adresse IP) dans la liste filtrée des charges de travail pour afficher la page Workload Profile (Profil de charge de travail).

Le tableau suivant décrit les champs affichés dans le tableau de l'état d'application.

Champ	Description
Nom de l'hôte	Nom d'hôte de la charge de travail.
Adresse	Les adresses IP de toutes les interfaces de la charge de travail
Enforcement Enabled	Indique si l'application est activée ou non sur l'agent.
Concrete Policies in Sync	Ceci indique si la version souhaitée de politiques concrètes est actuellement appliquée sur l'agent.
Politiques concrètes	Si cette valeur indique **Skipped** (ignoré) pour un hôte, cela signifie que la limite des politiques est atteinte pour l'agent sur cet hôte. (Consultez Limites liées aux politiques.)
Policy Count	Le nombre de politiques concrètes sur l'agent.
État	L'état de la dernière application de configuration de politiques. Si l'état est **CONFIG_SUCCESS**, cela indique que la version actuelle est appliquée sans problème.

État d'application pour les connecteurs infonuagiques

Si vous avez configuré les connecteurs infonuagiques AWS ou Azure :

L'état d'application de toutes les interfaces est affiché dans la page d'état d'application. Si les politiques sont appliquées avec succès, elles sont synchronisées, sinon les messages d'erreur correspondants s'affichent.

Le nombre de politiques dans la page d'état d'application est issu de la comptabilité Cisco Secure Workload, mais pas de la gestion de règles AWS ou Azure.

(AWS uniquement) Le champ de nom d'hôte sur cette page est dérivé du DNS public. Si le DNS public n'est pas activé sur le VPC donné, le champ de nom d'hôte est vide.

Suspendre les mises à jour des politiques

Caution Cette option met en pause les mises à jour de politiques pour TOUTES les charges de travail dans TOUTES les portées.

Cette fonctionnalité nécessite des privilèges d'administrateur de site ou de service d'assistance à la clientèle.

Pour suspendre les mises à jour des règles pour tous les points terminaux d'application dans toutes les portées :

1. Dans le volet de navigation, choisissez **Defend (Défendre)** > **Enforcement (Mise en application)** .
2. Cliquez sur l'état à côté de **Policy Updates** (Mises à jour des politiques) .
3. Lisez et acceptez la mise en garde.

Figure 3: Les règles de pare-feu sont mises à jour en permanence

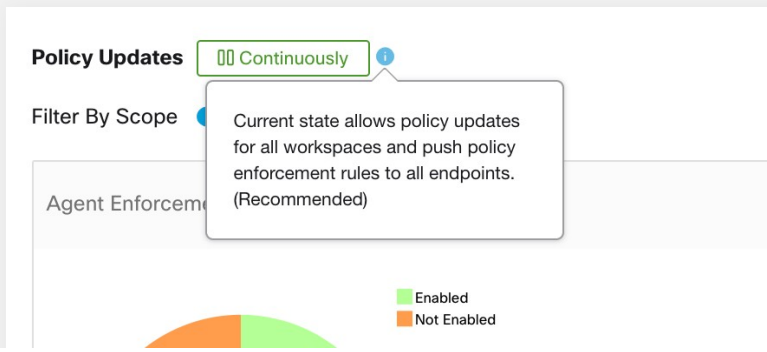


Figure 4: Les mises à jour des règles de pare-feu sont suspendues

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.