Configurer et gérer les connecteurs pour Cisco Secure Workload

Les connecteurs permettent à Cisco Secure Workload de s'intégrer à des ressources externes, telles que les commutateurs réseau, les routeurs, les pare-feu et les systèmes de gestion des terminaux, pour recueillir des données de télémétrie, acquérir des observations de flux et élargir le contexte de l'inventaire et des terminaux.

Que sont les connecteurs

Les connecteurs de Cisco Secure Workload sont des intégrations qui permettent à Cisco Secure Workload d'interagir avec diverses ressources et de recueillir des données à partir de diverses ressources à des fins différentes. Pour configurer et utiliser les connecteurs, dans le volet de navigation, choisissez **Manage (Gestion)** > **Connectors (Connecteurs)**.

Note Les connecteurs nécessitent une appliance virtuelle. Pour en savoir plus, consultez la section Appliances virtuelles pour les connecteurs.

Connecteurs pour l'acquisition de flux

Les connecteurs transmettent les observations de flux de différents commutateurs de réseau, routeurs et autres boîtiers intermédiaires (tels que les équilibreurs de charge et les pare-feu) à Cisco Secure Workload à des fins d'acquisition de flux.

Cisco Secure Workload prend en charge l'acquisition de flux par l'intermédiaire de NetFlow v9, IPfIX et des protocoles personnalisés. En plus des observations des flux, les connecteurs de boîtier intermédiaire relient les flux côté client et côté serveur pour comprendre quels flux client sont liés à quels flux serveur.

Connecteur	Description	Déployé sur une appliance virtuelle
NetFlow	Recueillez les données télémétriques NetFlow V9 ou IP-fIX à partir d'appareils réseau comme les routeurs et les commutateurs.	Acquisition de Cisco Secure Workload
F5 BIG-IP	Recueillez les données télémétriques de F5 BIG-IP, reliez les flux côté client et côté serveur, et enrichissez l'inventaire du client avec les attributs utilisateur.	Acquisition de Cisco Secure Workload
Citrix Netscaler	Recueillez la télémétrie de Citrix ADC, reliez des flux côté client et côté serveur.	Acquisition de Cisco Secure Workload
Pare-feu du connecteur sécurisé Cisco	Recueillez les données de télémétrie à partir de Cisco Secure Firewall ASA, de Cisco Secure Firewall Threat Defense, et reliez les flux côté client et côté serveur.	Acquisition de Cisco Secure Workload
Meraki	Recueillez les données de télémétrie des pare-feux Meraki.	Acquisition de Cisco Secure Workload
ERSPAN	Recueillir les données de télémétrie ERSPAN à partir de périphériques réseau qui prennent en charge ERSPAN	Acquisition de Cisco Secure Workload
Consultez aussi	connecteurs infonuagiques	–

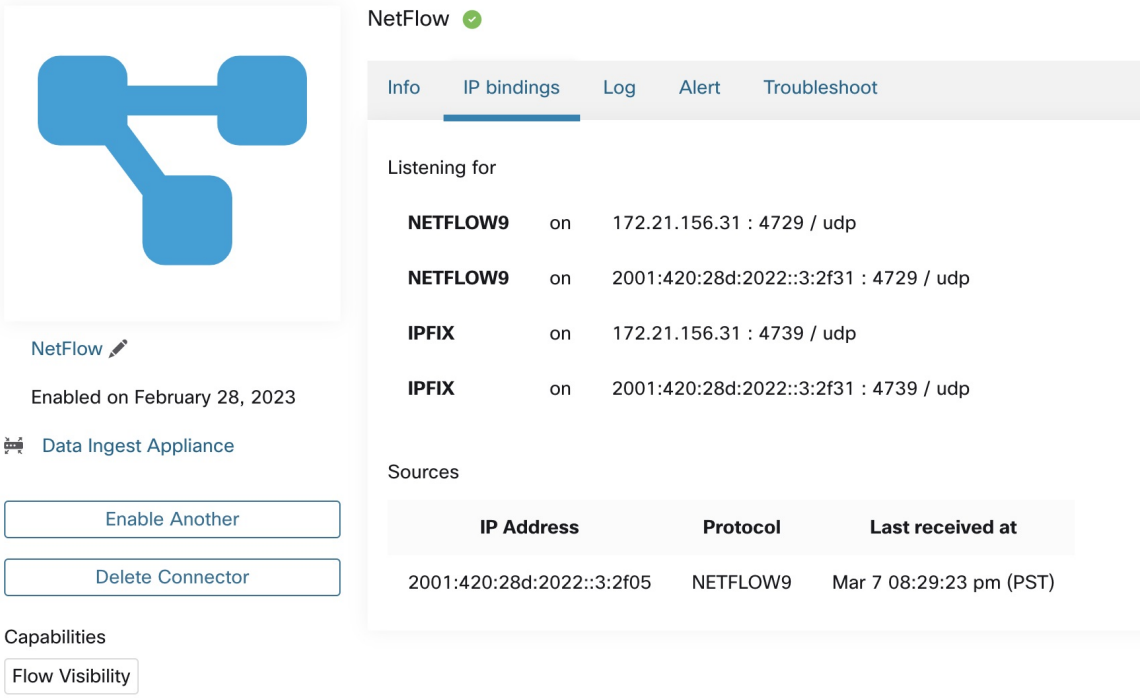
Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

Connecteur NetFlow

Le connecteur NetFlow permet à Cisco Secure Workload d'intégrer les observations de flux des routeurs et des commutateurs du réseau.

Cette solution permet aux hôtes d'éviter d'exécuter des agents logiciels, car les commutateurs Cisco relayent les enregistrements NetFlow à un connecteur NetFlow hébergé dans un appareil d'acquisition Cisco Secure Workload pour traitement.

Figure 1: Connecteur NetFlow



Qu'est-ce que NetFlow

Le protocole NetFlow permet aux routeurs et aux commutateurs d'agréger le trafic qui les traverse en flux et d'exporter ces flux vers un collecteur de flux.

Le collecteur de flux reçoit ces enregistrements de flux et les stocke pour les interroger et les analyser hors ligne. Les routeurs et commutateurs Cisco prennent en charge NetFlow.

En règle générale, la configuration comprend les étapes suivantes :

1. Activez la fonctionnalité NetFlow sur un ou plusieurs périphériques réseau et configurez les modèles de flux que les périphériques doivent exporter.
2. Configurez les informations de point terminal du collecteur NetFlow sur les périphériques réseau distants. Ce collecteur NetFlow est à l'écoute sur le point terminal configuré pour recevoir et traiter les enregistrements de flux NetFlow.

Acquisition de flux dans Cisco Secure Workload

Le connecteur NetFlow est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements de flux des périphériques réseau et les transfère à Cisco Secure Workload pour une analyse du flux. Vous pouvez activer un connecteur NetFlow sur un appareil d'acquisition Cisco Secure Workload et l'exécuter en tant que conteneur Docker.

Le connecteur NetFlow s'enregistre également auprès de Cisco Secure Workload en tant qu'agent NetFlow Cisco Secure Workload. Le connecteur NetFlow désencapsule les paquets de protocole NetFlow (c'est-à-dire les enregistrements de flux); traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Remarque Le connecteur NetFlow prend en charge les protocoles NetFlow v9 et IPFIX.

Remarque Chaque connecteur NetFlow ne doit signaler les flux que pour un seul VRF. Le connecteur exporte les flux et les place dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Secure Workload.

Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* (Configurations VRF à distance de l'agent), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur.

Le formulaire vous demande de fournir : le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Limitation de débit

Le connecteur NetFlow accepte jusqu'à 15 000 flux par seconde. Notez qu'un paquet NetFlow v9 ou IPFIX peut contenir un ou plusieurs enregistrements de flux et de modèle. Le connecteur NetFlow analyse les paquets et identifie les flux. Si le connecteur analyse plus de 15 000 flux par seconde, il abandonne les enregistrements de flux supplémentaires.

Notez également que le client Cisco Secure Workload ne prend en charge le connecteur NetFlow que si le débit se trouve dans cette limite acceptable.

Si le débit dépasse 15 000 flux par seconde, nous vous recommandons de commencer par régler le débit pour qu'il respecte les limites et de maintenir ce niveau pendant au moins trois jours (pour exclure les problèmes liés à un débit entrant plus élevé).

Si le problème persiste, le service d'assistance à la clientèle commence à examiner le problème et à identifier une solution de contournement et/ou une solution appropriée.

Éléments d'information pris en charge

Le connecteur NetFlow prend *uniquement* en charge les éléments d'information suivants dans les protocoles NetFlow v9 et IPFIX. Pour en savoir plus, consultez Entités IP Flow Information Export (IPFIX).

ID d'élément	Nom	Description	Obligatoire
1	octetDeltaCount	Nombre d'octets dans les paquets entrants pour ce flux.	Oui
2	packetDeltaCount	Nombre de paquets entrants pour ce flux.	Oui
4	protocolIdentifier	Valeur du numéro de protocole de l'en-tête du paquet IP.	Oui

ID d'élément	Nom	Description	Obligatoire
6	tcpControlBits	Bits de commande TCP observés pour les paquets de ce flux. L'agent gère les indicateurs FIN, SYN, RST, PSH, ACK et URG.	Non
7	sourceTransportPort	Identifiant du port source dans l'en-tête de transport.	Oui
8	sourceIPv4Address	Adresse source IPv4 dans l'en-tête du paquet IP.	8 ou 27
11	destinationTransportPort	Identifiant du port de destination dans l'en-tête de transport.	Oui
12	destinationIPv4Address	Adresse de destination IPv4 dans l'en-tête du paquet IP.	12 ou 28
27	sourceIPv6Address	Adresse source IPv6 dans l'en-tête du paquet IP.	8 ou 27
28	destinationIPv6Address	Adresse de destination IPv6 dans l'en-tête du paquet IP.	12 ou 28
150	flowStartSeconds	Horodatage absolu du premier paquet du flux (en secondes).	Non
151	flowEndSeconds	Horodatage absolu du dernier paquet du flux (en secondes).	Non
152	flowStartMilliseconds	Horodatage absolu du premier paquet du flux (en millisecondes).	Non
153	flowEndMilliseconds	Horodatage absolu du dernier paquet du flux (en millisecondes).	Non
154	flowStartMicroseconds	Horodatage absolu du premier paquet du flux (en microsecondes).	Non
155	flowEndMicroseconds	Horodatage absolu du dernier paquet du flux (en microsecondes).	Non

ID d'élément	Nom	Description	Obligatoire
156	flowStartNanoseconds	Horodatage absolu du premier paquet du flux (en nanosecondes).	Non
157	flowEndNanoseconds	Horodatage absolu du dernier paquet du flux (en nanosecondes).	Non

Comment configurer NetFlow sur le commutateur

Les étapes suivantes concernent un commutateur Nexus 9000. Les configurations peuvent différer légèrement pour les autres plateformes Cisco. Dans tous les cas, consultez le guide de configuration officiel de Cisco pour la plateforme Cisco que vous configurez.

Procedure

Étape 1 Entrer en mode de configuration globale.

```
switch# configure terminal
```

Étape 2 Activez la fonction NetFlow.

```
switch(config)# feature netflow
```

Étape 3 Configurez un enregistrement de flux.

L'exemple de configuration suivant montre comment générer des informations de cinq tuples d'un flux dans un enregistrement NetFlow.

```
switch(config)# flow record ipv4-records
switch(config-flow-record)# description IPv4Flow
switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match transport source-port
switch(config-flow-record)# match transport destination-port
switch(config-flow-record)# collect transport tcp flags
switch(config-flow-record)# collect counter bytes
switch(config-flow-record)# collect counter packets
```

Étape 4 Configurez un exportateur de flux.

L'exemple de configuration suivant précise la version du protocole NetFlow, l'intervalle d'échange du modèle NetFlow et les détails de point de terminaison du collecteur NetFlow. Préciser l'adresse IP et le port sur lesquels vous activez le connecteur NetFlow sur un appareil d'acquisition Cisco Secure Workload.

```
switch(config)# flow exporter flow-exporter-one
switch(config-flow-exporter)# description NetFlowv9ToNetFlowConnector
switch(config-flow-exporter)# destination 172.26.230.173 use-vrf management
switch(config-flow-exporter)# transport udp 4729
switch(config-flow-exporter)# source mgmt0
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# template data timeout 20
```

Étape 5 Configurez un moniteur de flux.

Créez un moniteur de flux et associez-le à un enregistrement de flux et à un exportateur de flux.

```
switch(config)# flow monitor ipv4-monitor
switch(config-flow-monitor)# description IPv4FlowMonitor
switch(config-flow-monitor)# record ipv4-records
switch(config-flow-monitor)# exporter flow-exporter-one
```

Étape 6 appliquez le moniteur de flux à une interface.

```
switch(config)# interface Ethernet 1/1
switch(config-if)# ip flow monitor ipv4-monitor input
```

Les étapes ci-dessus configurent NetFlow sur le Nexus 9000 pour exporter les paquets de protocole NetFlow v9 pour le trafic entrant passant par l'interface 1/1. Il envoie les enregistrements de flux au 172.26.230.173:4729 sur un protocole UDP. Chaque enregistrement de flux comprend des informations de cinq tuples du trafic et le nombre d'octets/paquets du flux.

Figure 2: Configuration d'exécution de NetFlow sur le commutateur Cisco Nexus 9000

```
switch# show running-config netflow

!Command: show running-config netflow
!Time: Wed Mar 21 04:25:21 2018

version 7.0(3)I7(1)
feature netflow

flow timeout 60
flow exporter flow-exporter-173
  destination 172.26.230.173 use-vrf management
  transport udp 4729
  source mgmt0
  version 9
    template data timeout 20
flow record ipv4-records
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match transport source-port
  match transport destination-port
  collect transport tcp flags
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
flow monitor ipv4-monitor
  record ipv4-records
  exporter flow-exporter-173


interface Ethernet1/1
  ip flow monitor ipv4-monitor input

interface Ethernet1/2
  ip flow monitor ipv4-monitor input

switch#
```

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Pour les connecteurs NetFlow, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs NetFlow sur un seul appareil d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs NetFlow sur un détenteur (portée racine)	10
Nombre maximal de connecteurs NetFlow sur Cisco Secure Workload	100

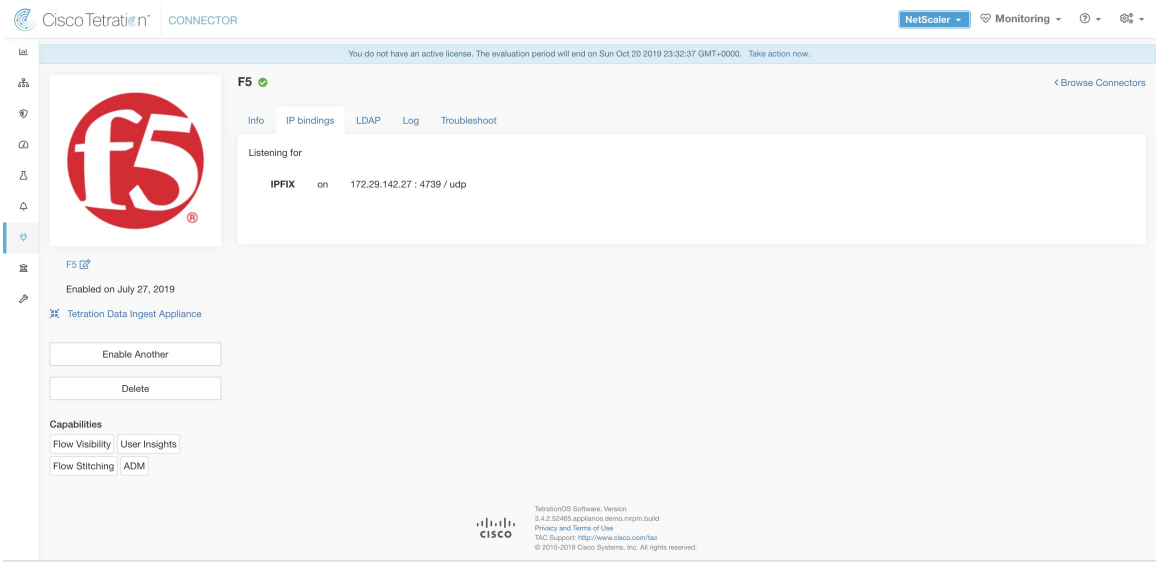
Connecteur F5

Le connecteur F5 permet à Cisco Secure Workload d'acquérir les observations de flux ADC F5 BIG-IP.

Il permet à Cisco Secure Workload de surveiller à distance les observations de flux sur les ADC F5 BIG-IP, d'assembler les flux côté client et côté serveur et d'annoter les utilisateurs sur les adresses IP clients (si les informations sur les utilisateurs sont disponibles).

Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les ADC F5 BIG-IP configurent l'exportation des enregistrements IPFIXvers le connecteur F5 pour traitement.

Figure 3: Connecteur F5



What is F5 BIG-IP IPFIX

F5 BIG-IP IPFIX logging collects flow data for traffic going through the F5 BIG-IP and exports IPFIX records to flow collectors.

Typically, the setup involves the following steps:

1. Create IPFIX Log-Publisher on F5 BIG-IP appliance.
2. Configure the IPFIX Log-Destination on the F5 BIG-IP appliance. This log-destination will be listening on configured endpoint to receive and process flow records.
3. Create an F5 iRule that publishes IPFIX flow records to the log-publisher.
4. Add the F5 iRule to the virtual server of interest.

Note F5 connector supports F5 BIG-IP software version 12.1.2 and above.

Acquisition de flux dans Cisco Secure Workload

Le connecteur F5 BIG-IP est principalement un collecteur IPFIX. Le connecteur reçoit les enregistrements de flux des CAN F5 BIG-IP, connecte les flux avec NAT et les transfère à Cisco Secure Workload pour une analyse des flux. En outre, si la configuration LDAP est fournie au connecteur F5, il détermine les valeurs des attributs LDAP configurés d'un utilisateur associé à la transaction (si F5 authentifie l'utilisateur avant de traiter la transaction). Les attributs sont associés à l'adresse IP du client où le flux s'est produit.

Remarque Le connecteur F5 prend uniquement en charge le protocole IPFIX.

Remarque Chaque connecteur F5 ne signale les flux que pour un VRF. Le connecteur place les flux qu'il exporte dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Cisco Secure Workload.

Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* (Configurations VRF à distance de l'agent), cliquez sur l'onglet *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire vous demande de fournir : le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

How to configure IPFIX on F5 BIG-IP

The following steps are for F5 BIG-IP load balancer. (Ref: Configuring F5 BIG-IP for IPFIX)

Purpose	Description
1. Create a pool of IPFIX collectors.	On F5 BIG-IP appliance, create the pool of IPFIX collectors. These are the IP addresses associated with F5 connectors on a Cisco Secure Workload Ingest appliance. F5 connectors run in Docker containers on the VM listen on port 4739 for IPFIX packets.
2. Create a log-destination.	The log destination configuration on F5 BIG-IP appliance specifies the actual pool of IPFIX collectors that should be used.
3. Create a log-publisher.	A log publisher specifies where F5 BIG-IP sends the IPFIX messages. The publisher is bound with a log-destination.
4. Add a F5 and Cisco Secure Workload approved iRule.	Secure Workload and F5 developed iRules that will export flow records to F5 connectors. These iRules will export complete information about a given transaction: including all the endpoints, byte and packet counts, flow start and end time (in milliseconds). F5 connectors will create 4 independent flows and match each flow with its related flow.
5. Add the iRule to the virtual server.	In the iRule settings of a virtual server, add the Secure Workload, approved iRule to the virtual server.

The above steps configures IPFIX on F5 BIG-IP load balancer to export IPFIX protocol packets for traffic going through the appliance. Here is a sample config of F5.

Figure 4: Running configuration of IPFIX on F5 BIG-IP load balancer

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm  pool ipfix-pool-1
ltm pool ipfix-pool-1 {
    members {
        10.28.118.6:ipfix {
            address 10.28.118.6
            session monitor-enabled
            state up
        }
    }
    monitor gateway_icmp
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config sys  log-config
sys log-config destination ipfix ipfix-collector-1 {
    pool-name ipfix-pool-1
    transport-profile udp
}
sys log-config publisher ipfix-pub-1 {
    destinations {
        ipfix-collector-1 { }
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

In the example above, flow records will be published to *ipfix-pub-1*. *ipfix-pub-1* is configured with log-destination *ipfix-collector-1* which sends the IPFIX messages to IPFIX pool *ipfix-pool-1*. *ipfix-pool-1* has 10.28.118.6 as one of the IPFIX collectors. The virtual server *vip-1* is configured with IPFIX iRule *ipfix-rule-1* which specifies the IPFIX template and how the template gets filled and sent.

- F5 and Cisco Secure Workload approved iRule for TCP virtual server can be found in the following file See L4 iRule for TCP virtual server.

F5 and Cisco Secure Workload approved iRule for UDP virtual server can be found in the following file.

- See L4 iRule for UDP virtual server.

F5 and Cisco Secure Workload approved iRule for HTTPS virtual server with authentication enabled can be found in the following file.

- See iRule for HTTPS virtual server.

Note Before using the iRule downloaded from this guide, please update the **log-publisher** to point to the log-publisher configured in the F5 connector where the iRule will be added.

Note F5 has published a GitHub repository, f5-tetration to help users get started with flow-stitching. The iRules for publishing IPFIX records to F5 connector for various protocol types are available at: f5-tetration/irules. Please visit this site for latest iRule definitions. In addition, F5 also developed a script to: (1) install the correct iRule for the virtual servers, (2) add a pool of IPFIX collector endpoints (where F5 connectors listen for IPFIX records), (3) configure the log-collector and log-publisher, and (4) bind the correct iRule to the virtual servers. This tool minimizes manual configuration and user error while enabling flow-stitching use-case. The script is available at f5-tetration/scripts.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs.

Les configurations suivantes sont autorisées sur le connecteur.

- LDAP : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour choisir l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

En outre, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande qui peut être exécutée sur le conteneur. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

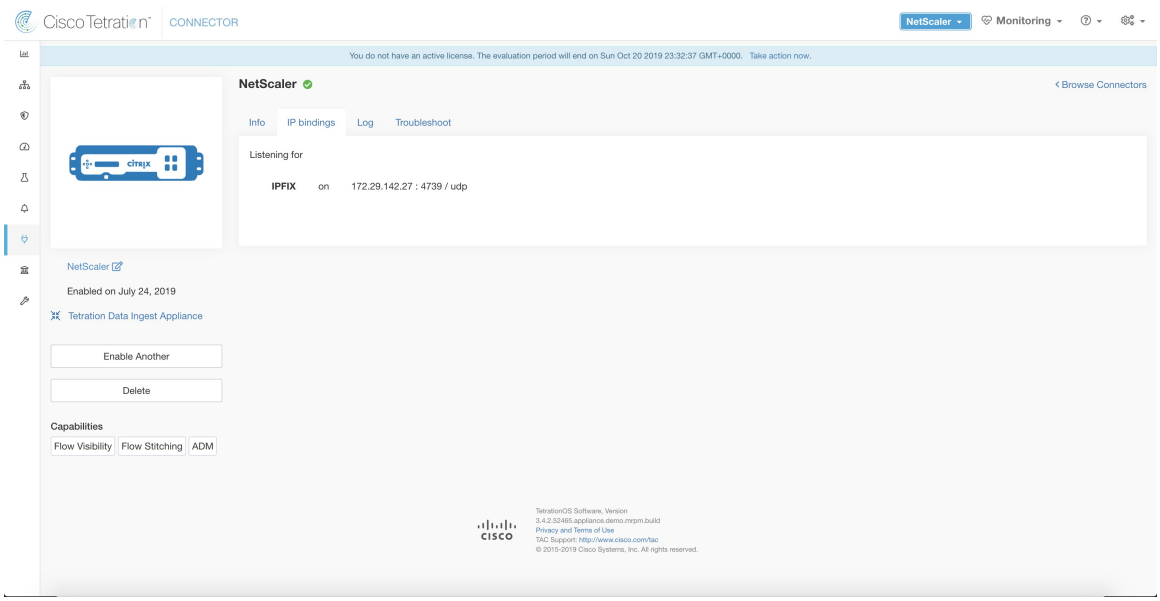
Limites

Unité	Limite
Nombre maximal de connecteurs F5 sur un dispositif d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs F5 sur un détenteur (portée racine)	10
Nombre maximal de connecteurs F5 sur Cisco Secure Workload	100

Connecteur NetScaler

Le connecteur NetScaler permet à Cisco Secure Workload d'acquérir les observations de flux des ADC Citrix (Citrix NetScalers). Il permet à Cisco Secure Workload de surveiller à distance les observations de flux sur les ADC Citrix et d'assembler les flux côté client et côté serveur. Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les ADC Citrix sont configurés pour exporter les enregistrements IPfFIX vers le connecteur NetScaler pour traitement.

Figure 5: Connecteur NetScaler



What is Citrix NetScaler AppFlow

Citrix NetScaler AppFlow collects flow data for traffic going through the NetScaler and exports IPFIX records to flow collectors. Citrix AppFlow protocol uses IPFIX to export the flows to flow collectors. Citrix AppFlow is supported in Citrix NetScaler load balancers.

Typically, the setup involves the following steps:

1. Enable AppFlow feature on one or more Citrix NetScaler instances.
2. Configure the AppFlow collector endpoint information on the remote network devices. This AppFlow collector will be listening on configured endpoint to receive and process flow records.
3. Configure AppFlow actions and policies to export flow records to AppFlow collectors.

Note NetScaler connector supports Citrix ADC software version 11.1.51.26 and above.

Acquisition de flux dans Cisco Secure Workload

Le connecteur NetScaler est essentiellement un collecteur Citrix AppFlow (IPFIX). Le connecteur reçoit les enregistrements de flux des ADC Citrix, regroupe les flux avec NAT et les transfère à Cisco Secure Workload pour une analyse des flux. Un connecteur NetScaler peut être activé sur un appareil d'acquisition Cisco Cisco Secure Workload et s'exécute en tant que conteneur Docker. Le connecteur NetScaler s'enregistre également auprès de Cisco Secure Workload en tant qu'agent NetScaler Cisco Secure Workload.

Note Le connecteur NetScaler prend uniquement en charge le protocole IPFIX.

Note Chaque connecteur NetScaler ne doit signaler les flux que pour un seul VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration du VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet Configuration. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

How to configure AppFlow on NetScaler

The following steps are for NetScaler load balancer. (Ref: Configuring AppFlow)

Procedure

Étape 1 Enable AppFlow on NetScaler.

```
enable ns feature appflow
```

Étape 2 Add AppFlow collector endpoints.

The collector receives the AppFlow records from NetScaler. Please specify the IP and port of NetScaler connector enabled on a Cisco Secure Workload Ingest appliance as an AppFlow collector.

```
add appflow collector c1 -IPAddress 172.26.230.173 -port 4739
```

Étape 3 Configure an AppFlow action.

This lists the collectors that will get AppFlow records if the associated AppFlow policy matches.

```
add appflow action a1 -collectors c1
```

Étape 4 Configure an AppFlow policy.

This is a rule that has to match for an AppFlow record to be generated.

```
add appflow policy p1 CLIENT.TCP.DSTPORT(22) a1
add appflow policy p2 HTTP.REQ.URL.SUFFIX.EQ("jpeg") a1
```

Étape 5 Bind AppFlow policy to Virtual Server.

Traffic hitting the IP of the virtual server (VIP) will be evaluated for AppFlow policy matches. On a match, a flow record is generated and sent to all collectors listed in the associated AppFlow action.

```
bind lb vserver lb1 -policyname p1 -priority 10
```

Étape 6 Optionally, bind AppFlow policy globally (for all virtual servers).

An AppFlow policy could also be bound globally to all virtual servers. This policy applies to all traffic that flows through Citrix ADC.

```
bind appflow global p2 1 NEXT -type REQ_DEFAULT
```

Étape 7 Optionally, template refresh interval.

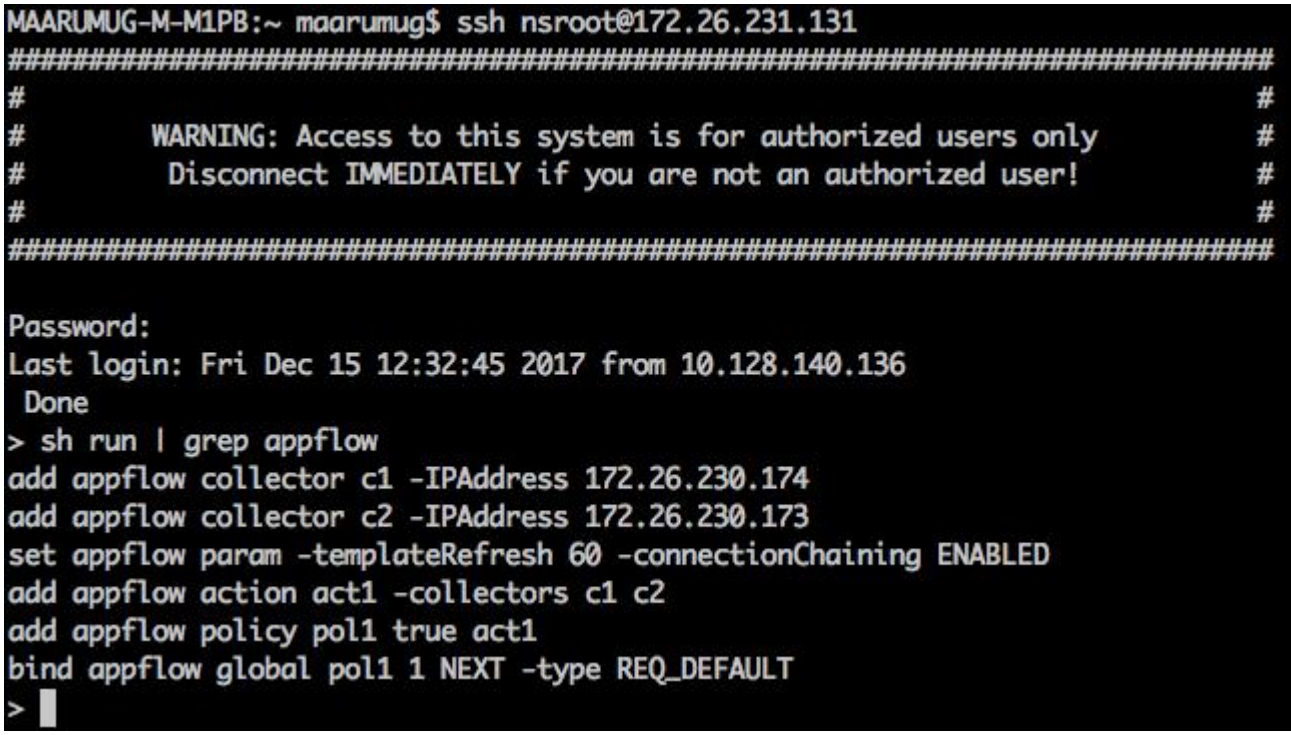
Default value for template refresh is 60 seconds.

```
set appflow param -templatereferesh 60
```

The above steps configures AppFlow on Citrix NetScaler load balancer to export IPFIX protocol packets for traffic going through NetScaler. The flow records will be sent to either 172.26.230.173:4739 (for traffic going through vserver lb1) and to 172.26.230.184:4739 (for all traffic going through the NetScaler). Each flow record includes 5 tuple information of the traffic and the byte/packet count of the flow.

The following screenshot shows a running configuration of AppFlow on a Citrix NetScaler load balancer.

Figure 6: Running configuration of AppFlow on Citrix NetScaler load balancer



Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour

et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. . Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

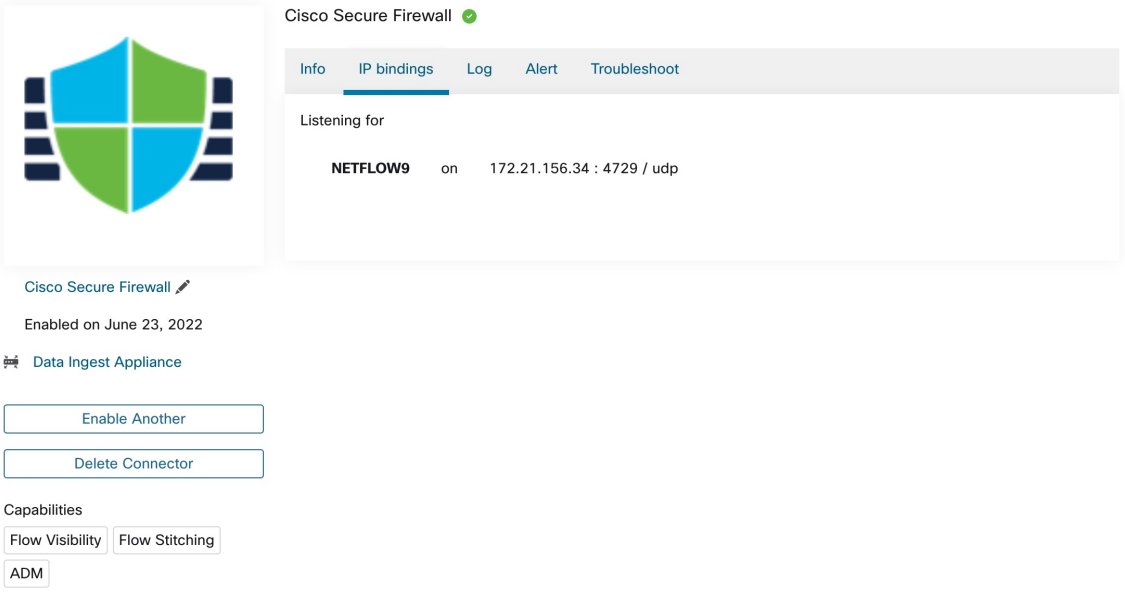
Tableau 1 : Limites

Unité	Limite
Nombre maximal de connecteurs NetScaler sur un appareil d'acquisition Cisco Secure Workload	3
Nombre maximal de connecteurs NetScaler sur un détenteur (portée racine)	10
Nombre maximal de connecteurs NetScaler sur Cisco Secure Workload	100

Cisco Secure Firewall Connector

Secure Firewall Connector (formerly known as ASA Connector) allows Cisco Secure Workload to ingest flow observations from Secure Firewall ASA (formerly known as Cisco ASA) and Secure Firewall Threat Defense (formerly known as Firepower Threat Defense or FTD). Using this solution, the hosts do not need to run software agents, because the Cisco switches will relay NetFlow Secure Event Logging (NSEL) records to Secure Firewall Connector hosted in a Cisco Secure Workload Ingest appliance for processing.

Figure 7: Secure Firewall Connector



Cisco Secure Firewall ASA NetFlow Secure Event Logging (NSEL) provides a stateful, IP flow monitoring that exports significant events in a flow to a NetFlow collector. When an event causes a state change on a

flow, an NSEL event is triggered that sends the flow observation along with the event that caused the state change to the NetFlow collector. The flow collector receives these flow records and stores them in their flow storage for offline querying and analysis.

Typically, the setup involves the following steps:

1. Enable NSEL feature on Secure Firewall ASA and/or Secure Firewall Threat Defense.
2. Configure the Secure Firewall connector endpoint information on Secure Firewall ASA and/or Secure Firewall Threat Defense. Secure Firewall connector will be listening on configured endpoint to receive and process NSEL records.

Acquisition de flux dans Cisco Secure Workload

Le connecteur de Cisco Secure Firewall est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements NSEL de Cisco Secure Firewall ASA et de Cisco Secure Firewall Threat Defense et les transmet à Cisco Secure Workload pour analyse du flux. Le connecteur de Cisco Secure Firewall peut être activé sur un appareil d'acquisition Cisco Secure Workload et s'exécute en tant que conteneur Docker.

Le connecteur de Cisco Secure Firewall s'enregistre également auprès de Cisco Secure Workload en tant qu'agent Cisco Secure Workload. Le connecteur de Cisco Secure Firewall désencapsule les paquets de protocole NSEL (c.-à-d. les enregistrements de flux). traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Note Le connecteur de Cisco Secure Firewall prend en charge le protocole NetFlow v9.

Note Chaque connecteur Cisco Secure Firewall ne doit signaler les flux que pour un seul VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Gestion des événements NSEL

Le tableau suivant montre comment les divers événements NSEL sont gérés par le connecteur Secure Firewall. Pour en savoir plus sur ces éléments, consultez le document Entités d'exportation d'informations sur les flux IP (IPFIX).

ID de l'élément de l'événement de flux : 233 Nom de l'élément : *NF_F_FW_EVENT*	Événement de flux étendu ID de l'élément : 33002 Nom de l'élément : *NF_F_FW_EXT_EVENT*	Action sur le connecteur de Cisco Secure Firewall
0 (par défaut, ignorez cette valeur)	Ce n'est pas important	Aucune opération
1 (Flux créé)	Ce n'est pas important	Envoyer le flux à Cisco Secure Workload

ID de l'élément de l'événement de flux : 233 Nom de l'élément : *NF_F_FW_EVENT*	Événement de flux étendu ID de l'élément : 33002 Nom de l'élément : *NF_F_FW_EXT_EVENT*	Action sur le connecteur de Cisco Secure Firewall
2 (Flux supprimé)	> 2000 (indique le motif de fin)	Envoyer le flux à Cisco Secure Workload
3 (Flux refusé)	1001 (refusé par la liste de contrôle d'accès d'entrée)	Envoyer le flux avec le statut rejeté à Cisco Secure Workload
	1002 (refusé par la liste de contrôle d'accès de sortie)	
	1003 (connexion refusée par l'interface ASA ou ICMP(v6) refusé au périphérique)	
	1004 (le premier paquet sur TCP n'est pas SYN)	
4 (Alerte de flux)	Ce n'est pas important	Aucune opération
5 (Flux mis à jour)	Ce n'est pas important	Envoyer le flux à Cisco Secure Workload

Basé sur l'enregistrement NSEL, le connecteur de Cisco Secure Firewall envoie l'observation de flux à Cisco Secure Workload. Les enregistrements de flux de la NSEL sont bidirectionnels. Ainsi, le connecteur Cisco Secure Firewall envoie deux flux : le flux aller et le flux inverse vers Cisco Secure Workload.

Voici les détails sur l'observation de flux envoyées par le connecteur de Cisco Secure Firewall à Cisco Secure Workload.

Observation du flux aller

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Source Port (port source)	7	*NF_F_SRC_PORT*
Adresse de destination	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Destination Port (port de destination)	11	*NF_F_DST_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	231	*NF_F_FWD_FLOW_DELTA_BYTES*

Champ	ID d'élément NSEL	Nom d'élément NSEL
Nombre de paquets	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Information de flux inverse

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
Source Port (port source)	11	*NF_F_DST_PORT*
Adresse de destination	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
Destination Port (port de destination)	7	*NF_F_SRC_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	232	*NF_F_REV_FLOW_DELTA_BYTES*
Nombre de paquets	299	*NF_F_REV_FLOW_DELTA_PACKETS*

NAT

Si le flux client vers ASA est avec NAT, les enregistrements de flux NSEL indiquent l'adresse IP/le port avec NAT du côté serveur. Le connecteur de Cisco Secure Firewall utilise ces informations pour relier les flux du serveur à l'ASA et de l'ASA au client.

Voici l'enregistrement de flux avec NAT vers l'avant.

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Source Port (port source)	227	*NF_F_XLATE_SRC_PORT*
Adresse de destination	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Destination Port (port de destination)	228	*NF_F_XLATE_DST_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*

Champ	ID d'élément NSEL	Nom d'élément NSEL
Nombre d'octets	231	*NF_F_FWD_FLOW_DELTA_BYTES*
Nombre de paquets	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

Le flux aller sera marqué comme étant lié à l'enregistrement de flux avec NAT dans la direction aller (et vice versa).

Voici l'enregistrement de flux avec NAT dans le sens inverse

Champ	ID d'élément NSEL	Nom d'élément NSEL
Protocole	4	*NF_F_PROTOCOL*
Adresse de la source	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
Source Port (port source)	228	*NF_F_XLATE_DST_PORT*
Adresse de destination	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
Destination Port (port de destination)	227	*NF_F_XLATE_SRC_PORT*
Heure de début du flux	152	*NF_F_FLOW_CREATE_TIME_MSEC*
Nombre d'octets	232	*NF_F_REV_FLOW_DELTA_BYTES*
Nombre de paquets	299	*NF_F_REV_FLOW_DELTA_PACKETS*

Le flux inverse sera marqué comme étant lié à l'enregistrement du flux avec NAT dans la direction inverse (et vice versa).

Note Seuls les ID d'élément NSEL répertoriés dans cette section sont pris en charge par le connecteur Cisco Secure Firewall.

Heuristique des indicateurs TCP

Les enregistrements NSEL ne contiennent pas d'information sur les indicateurs TCP. Le connecteur Cisco Secure Firewall utilise la méthode heuristique suivante pour définir les indicateurs TCP afin que les flux puissent être analysés de manière plus approfondie par la recherche automatique de politiques :

- S'il y a au moins un paquet de transfert, ajoute `SYN` aux indicateurs TCP de flux aller.
- S'il y a au moins deux paquets aller et un paquet retour, ajoute `ACK` aux indicateurs TCP de flux aller et `SYN-ACK` aux indicateurs TCP de flux inverse.
- Si la condition précédente est vérifiée et que l'événement de flux est Flux supprimé, ajoute `FIN` aux indicateurs TCP aller et arrière.

How to Configure NSEL on Secure Firewall ASA

The following steps are guidelines on how to configure NSEL and export NetFlow packets to a collector (i.e., Secure Firewall connector). Please also refer to the official Cisco configuration guide at Cisco Secure Firewall ASA NetFlow Implementation Guide for more details.

Here is an example NSEL configuration.

```
flow-export destination outside 172.29.142.27 4729
flow-export template timeout-rate 1
!
policy-map flow_export_policy
  class class-default
  flow-export event-type flow-create destination 172.29.142.27
  flow-export event-type flow-teardown destination 172.29.142.27
  flow-export event-type flow-denied destination 172.29.142.27
  flow-export event-type flow-update destination 172.29.142.27
  user-statistics accounting
service-policy flow_export_policy global
```

In this example, Secure Firewall ASA appliance is configured to sent NetFlow packets to *172.29.142.27* on port *4729*. In addition, *flow-export* actions are enabled on *flow-create*, *flow-teardown*, *flow-denied*, and *flow-update* events. When these flow events occur on ASA, a NetFlow record is generated and sent to the destination specified in the configuration.

Assuming a Secure Firewall connector is enabled on Cisco Secure Workload and listening on *172.29.142.27:4729* in a Cisco Secure Workload Ingest appliance, the connector will receive NetFlow packets from Secure Firewall ASA appliance. The connector processes the NetFlow records as discussed in Gestion des événements NSELand exports flow observations to Secure Workload. In addition, for NATed flows, the connector stitches the related flows (client-side and server-side) flows.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

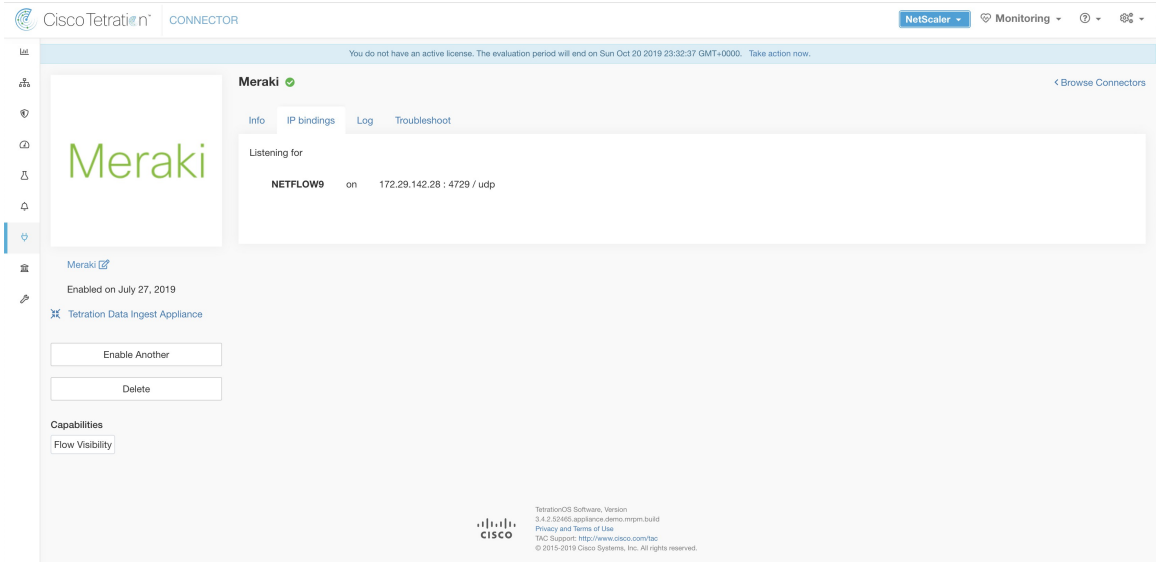
Unité	Limite
Nombre maximal de connecteurs Cisco Secure Firewall sur un dispositif d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs Cisco Secure Firewall sur un détenteur (portée racine)	10

Unité	Limite
Nombre maximal de connecteurs Cisco Secure Firewall sur Cisco Secure Workload	100

Connecteur Meraki

Le connecteur Meraki permet à Cisco Secure Workload d'acquérir les observations de flux des pare-feu Meraki (inclus dans les appareils de sécurité et les points d'accès sans fil Meraki MX). Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter des agents logiciels, car les commutateurs Cisco relayent les enregistrements NetFlow au connecteur Meraki hébergé dans un appareil d'acquisition Cisco Secure Workload pour le traitement.

Figure 8: Connecteur Meraki



Qu'est-ce que NetFlow

Le protocole NetFlow permet aux périphériques réseau comme le pare-feu Meraki d'agréger le trafic qui les traverse en flux et d'exporter ces flux vers un collecteur de flux. Le collecteur de flux reçoit ces enregistrements de flux et les stocke pour les interroger et les analyser hors ligne.

En règle générale, la configuration comprend les étapes suivantes :

1. Activer les rapports statistiques NetFlow sur le pare-feu Meraki.
2. Configurez les informations de point terminal du collecteur NetFlow sur le pare-feu Meraki.

Acquisition de flux dans Cisco Secure Workload

Le connecteur Meraki est essentiellement un collecteur NetFlow. Le connecteur reçoit les enregistrements de flux des pare-feu Meraki configurés pour exporter les statistiques de trafic NetFlow. Il traite les enregistrements NetFlow et envoie les observations de flux signalées par les pare-feu Meraki à Cisco Secure Workload pour une analyse de flux. Un connecteur Meraki peut être activé sur un appareil d'acquisition Cisco Secure Workload et s'exécute en tant que conteneur Docker.

Le connecteur Meraki s'enregistre également auprès de Cisco Secure Workload en tant qu'agent Meraki Cisco Secure Workload. Le connecteur Meraki désencapsule les paquets de protocole NetFlow (c.-à-d. les enregistrements de flux); traite ensuite les flux et les signale comme un agent Cisco Secure Workload normal. Contrairement à un agent de visibilité approfondie, il ne signale aucune information sur le processus ou l'interface.

Note Le connecteur Meraki prend en charge le protocole NetFlow v9.

Note Chaque connecteur Meraki ne doit signaler les flux que pour un VRF. Les flux exportés par le connecteur sont placés dans le VRF en fonction de la configuration VRF de l'agent dans la grappe Cisco Secure Workload. Pour configurer le VRF pour le connecteur, accédez à : **Manage (Gestion)** > **Agents (Agents)**, puis cliquez sur l'onglet **Configuration**. Dans cette page, sous la section *Agent Remote VRF Configurations* Configurations VRF d'agents distants), cliquez sur *Create Config* (Créer une configuration) et fournissez les détails du connecteur. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP du connecteur et la plage de numéros de port qui peut potentiellement envoyer des enregistrements de flux à la grappe.

Gestion des enregistrements NetFlow

Selon l'enregistrement NetFlow, le connecteur Meraki envoie l'observation de flux à Cisco Secure Workload. Les enregistrements de flux Meraki NetFlow sont bidirectionnels. Ainsi, le connecteur Meraki envoie deux flux : le flux aller et le flux inverse à Cisco Secure Workload.

Voici les détails sur l'observation de flux envoyée par le connecteur Meraki à Cisco Secure Workload.

Observation du flux aller

Champ	ID d'élément	Nom de l'élément
Protocole	4	*protocolIdentifier*
Adresse de la source	8	*sourceIPv4Address*
Source Port (port source)	7	*sourceTransportPort*
Adresse de destination	12	*destinationIPv4Address*
Destination Port (port de destination)	11	*destinationTransportPort*
Nombre d'octets	1	*octetDeltaCount*
Nombre de paquets	2	*packetDeltaCount*
Heure de début du flux		Défini en fonction du moment de la réception de l'enregistrement NetFlow pour ce flux sur le connecteur

Information de flux inverse

Champ	ID d'élément	
Protocole	4	*protocolIdentifier*
Adresse de la source	8	*sourceIPv4Address*
Source Port (port source)	7	*sourceTransportPort*
Adresse de destination	12	*destinationIPv4Address*
Destination Port (port de destination)	11	*destinationTransportPort*
Nombre d'octets	23	*postOctetDeltaCount*
Nombre de paquets	24	*postPacketDeltaCount*
Heure de début du flux		Défini en fonction du moment de la réception de l'enregistrement NetFlow pour ce flux sur le connecteur

Comment configurer NetFlow sur un pare-feu Meraki

Les étapes suivantes montrent comment configurer les rapports NetFlow sur le pare-feu Meraki.

Procedure

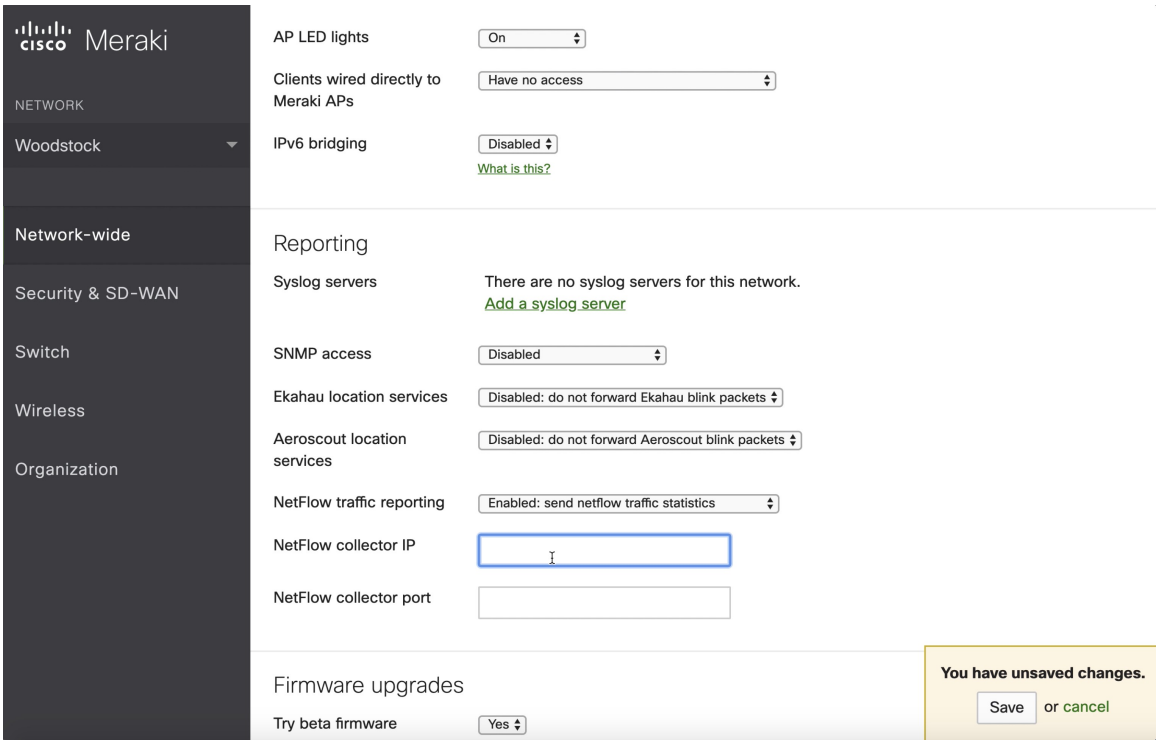
Étape 1 Connectez-vous à la console de l'interface utilisateur Meraki.

Étape 2 Naviguez jusqu'à **Network-wide (À l'échelle du réseau)** > **General (Général)**. Dans les paramètres de *rapport*, activez **les rapports sur le trafic NetFlow** et assurez-vous que la valeur est définie sur *Activé : envoyer les statistiques de trafic NetFlow.*

Étape 3 Réglez **NetFlow collector IP** (adresse IP du collecteur NetFlow) et **NetFlow collector port** (port du collecteur NetFlow) sur l'adresse IP et le port sur lesquels le connecteur Meraki écoute dans le dispositif d'acquisition Cisco Secure Workload. Le port par défaut sur lequel le connecteur Meraki écoute les enregistrements NetFlow est 4729.

Étape 4 Enregistrer les modifications

Figure 9: Activation de NetFlow sur un pare-feu Meraki



Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

En outre, les ports d'écoute du protocole NetFlow v9 sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs Meraki sur un dispositif d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs Meraki sur un détenteur (portée racine)	10

Unité	Limite
Nombre maximal de connecteurs Meraki sur Cisco Secure Workload	100

Connecteur ERSPAN

Le connecteur ERSPAN permet à Cisco Secure Workload d'acquérir les observations de flux des routeurs et des commutateurs du réseau. Grâce à cette solution, les hôtes n'ont pas besoin d'exécuter d'agents logiciels, car les commutateurs Cisco relayent le trafic des hôtes vers le connecteur ERSPAN pour traitement.

Qu'est-ce qu'ERSPAN?

L'analyseur ERSPAN (Encapsulating Remote Switch Port Analyzer) est une fonctionnalité présente dans la plupart des commutateurs Cisco. Il reproduit les trames vues par un périphérique réseau, les encapsule dans un paquet IP et les envoie à un analyseur distant. Les utilisateurs peuvent sélectionner une liste d'interfaces ou de VLAN sur le commutateur à surveiller.

En général, l'installation consiste à configurer la ou les sessions de surveillance ERSPAN de source sur un ou plusieurs périphériques de réseau et à configurer la ou les sessions de surveillance ERSPAN de destination sur le ou les périphériques de réseau distants directement connectés à un analyseur de trafic.

Le connecteur ERSPAN Cisco Secure Workload fournit à la fois la session ERSPAN de destination et les fonctionnalités d'analyse du trafic; il n'est donc pas nécessaire de configurer des sessions de destination sur les commutateurs dotés de la solution Cisco Secure Workload.

Que sont les agents SPAN

Chaque connecteur ERSPAN enregistre un agent SPAN auprès de la grappe. Les agents SPAN Cisco Secure Workload sont des agents Cisco Secure Workload standard configurés pour traiter uniquement les paquets ERSPAN : à l'instar des sessions ERSPAN de destination de Cisco, ils désencapsulent les trames en miroir; ils traitent ensuite les flux et en rendent compte comme un agent Cisco Secure Workload normal. Contrairement aux agents de visibilité approfondie, ils ne signalent aucune information sur les processus ou l'interface.

Qu'est-ce que l'appareil d'acquisition pour ERSPAN

L'appareil d'acquisition Cisco Secure Workload pour ERSPAN est une machine virtuelle qui fait fonctionner en interne trois connecteurs ERSPAN Cisco Secure Workload. Il utilise le même OVA ou QCOW2 que l'appareil d'acquisition classique.

Chaque connecteur s'exécute dans un conteneur Docker dédié auquel une vNIC et deux cœurs vCPU sans quota de limite sont exclusivement affectés.

Le connecteur ERSPAN enregistre un agent SPAN avec la grappe avec le nom d'hôte du conteneur :<Nom d'hôte de la machine virtuelle> -<Adresse IP de l'interface>.

Les connecteurs et les agents sont conservés ou restaurés lors du blocage ou du redémarrage de la machine virtuelle, du daemon ou du conteneur Docker.

Remarque L'état du connecteur ERSPAN est renvoyé à la page Connector (connecteur). Consultez la page Agent List (Liste des agents) et vérifiez l'état des agents SPAN correspondants.

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs. Pour les connecteurs ERSPAN, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Comment configurer la session ERSPAN source

Les étapes suivantes concernent un commutateur Nexus 9000. Les configurations peuvent différer légèrement pour les autres plateformes Cisco. Pour la configuration d'une plateforme Cisco, consultez le Guide de l'utilisateur du Cisco Secure Workload.

Illustration 10 : Configurer la source ERSPAN sur Cisco Nexus 9000

```
Enter the configuration mode
# config terminal

Configure the erspan source IP address
(config)# monitor erspan origin ip-address 172.28.126.1 global

Create and configure the source erspan session
(config)# monitor session 10 type erspan-source
(config-erspan-src)# source interface ethernet 1/23 both
(config-erspan-src)# source vlan 315, 512
(config-erspan-src)# destination ip 172.28.126.194

Turn on the monitor session
(config-erspan-src)# no shut

Persist the configuration
# copy runnin-config startup-config
```

Les étapes ci-dessus ont créé une session ERSPAN source avec l'ID 10. Le commutateur mettra en miroir les trames entrant et sortant (à la fois) de l'interface eth1/23 et de celles sur les VLANS 315 et 512. Le paquet GRE externe transportant la trame miroir aura l'IP source 172.28.126.1 (doit être l'adresse d'une interface L3 sur ce commutateur) et l'IP de destination 172.28.126.194. Il s'agit de l'une des adresses IP configurées sur la machine virtuelle ERSPAN.

Formats ERSPAN pris en charge

Les agents SPAN Cisco Secure Workload peuvent traiter les paquets ERSPAN de type I, II et II décrits dans la RFC ERSPANproposée. Par conséquent, ils peuvent traiter les paquets ERSPAN générés par les périphériques Cisco. Parmi les formats non conformes à la RFC, ils peuvent traiter les paquets ERSPAN générés par VMware vSphere Distributed Switch (VDS).

Considérations relatives aux performances lors de la configuration de la source ERSPAN

Choisissez avec soin la liste de ports/VLAN de la source ERSPAN. Bien que l'agent SPAN dispose de deux vCPU dédiés, la session peut générer une quantité considérable de paquets, ce qui pourrait saturer la puissance de traitement de l'agent. Si un agent reçoit plus de paquets qu'il ne peut en traiter, cela sera indiqué dans le graphique Paquets manquants de l'agent sur la page Deep Visibility Agent (Agent de visibilité approfondie) de la grappe.

Un réglage plus fin des trames sur lesquelles la source ERSPAN sera mise en miroir peut être obtenu à l'aide de politiques ACL, généralement à l'aide du mot-clé de configuration filter.

Si le commutateur le prend en charge, la session source ERSPAN peut être configurée pour modifier l'unité de transport maximale (MTU) du paquet ERSPAN (généralement la valeur par défaut de 1500 octets), généralement au moyen d'un mot-clé mtu. La diminuer limitera l'utilisation de la bande passante ERSPAN dans votre infrastructure réseau, mais n'aura aucun effet sur la charge de l'agent SPAN, étant donné que la charge de travail de l'agent est par paquet. Lorsque vous réduisez cette valeur, prévoyez de la place pour 160 octets pour la trame miroir. Pour plus de détails sur le surdébit d'en-tête ERSPAN, consultez la demande d'informations sur ERSPAN RFCproposée.

Il existe trois versions d'ERSPAN. Plus la version est petite, plus le surdébit de l'en-tête ERSPAN est faible. Les versions II et III permettent d'appliquer des politiques de qualité de service (QoS) aux paquets ERSPAN et fournissent des renseignements sur le VLAN. La version III comporte encore plus de paramètres. La version II est généralement celle par défaut des commutateurs Cisco. Bien que les agents ERSPAN Cisco Secure Workload prennent en charge les trois versions, pour le moment ils n'utilisent aucune information supplémentaire que transportent les paquets ERSPAN versions II et III.

Questions de sécurité.

Le système d'exploitation invité de la machine virtuelle d'acquisition pour ERSPAN est CentOS 7.9, dont les paquets serveur/clients OpenSSL ont été supprimés.

Remarque CentOS 7.9 est le système d'exploitation invité pour les appareils virtuels d'acquisition et de périphérie de Cisco Secure Workload 3.8.1.19 et les versions antérieures. À partir de la version 3.8.1.36 de Cisco Secure Workload, le système d'exploitation est AlmaLinux 9.2.

Une fois que la machine virtuelle est démarrée et que les conteneurs d'agents SPAN sont déployés (l'opération prend quelques minutes lors du premier démarrage uniquement), aucune interface réseau, hormis la boucle avec retour, ne sera présente dans la machine virtuelle. Par conséquent, la seule façon d'accéder à l'appareil est via sa console.

L'interface réseau de la machine virtuelle est maintenant déplacée à l'intérieur des conteneurs Docker. Les conteneurs exécutent une image Docker basée sur centos : 7.9.2009 sans port TCP/UDP ouvert.

Remarque À partir de la version 3.8.1.36 de Cisco Secure Workload, les conteneurs exécutent almalinux/9-base:9.2.

En outre, les conteneurs sont exécutés avec les privilèges de base (option no –privileged) plus la capacité NET_ADMIN.

Dans le cas improbable où un conteneur serait contaminé, le système d'exploitation invité de la machine virtuelle ne devrait pas pouvoir être contaminé depuis l'intérieur du conteneur.

Toutes les autres considérations de sécurité valides pour les agents Cisco Secure Workload exécutés dans un hôte s'appliquent également aux agents SPAN Cisco Secure Workload exécutés dans les conteneurs Docker.

Dépannage

Une fois que les agents SPAN sont à l'état actif dans la page Monitoring/Agent Overview (Surveillance/Aperçu de l'agent) de la grappe, aucune action n'est nécessaire sur la machine virtuelle ERSPAN et l'utilisateur n'a pas besoin de s'y connecter. Si cela ne se produit pas ou si les flux ne sont pas signalés à la grappe, les renseignements suivants permettront d'identifier les problèmes de déploiement.

Dans des conditions normales, sur la machine virtuelle :

- `systemctl status tet_vm_setup` signale un service *inactif* avec l'état de sortie *SUCCESS*;
- `systemctl status tet-nic-driver` signale un service *actif*;
- `docker network ls` signale cinq réseaux : `host, none` et trois `erspan-<iface name>;`
- `ip link` signale uniquement l'interface de boucle avec retour;
- `docker ps` signale trois conteneurs en cours d'exécution;
- `docker logs <cid>` pour chaque conteneur, contient le message :`NFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)` (Succès du NFO : le capteur tet est entré dans l'état RUNNING, le processus est resté en place pendant > 1 seconde (startsecs).
- `docker exec <cid> ifconfig` ne signale qu'une seule interface, en plus de la boucle avec retour;
- `docker exec <cid> route -n` signale la passerelle par défaut;
- `docker exec <cid> iptables -t raw -S PREROUTING` signale la règle `-A PREROUTING-p gre -j DROP;`

Si l'un des éléments ci-dessus n'est pas vérifié, vérifiez les journaux du script de déploiement dans `/local/tetration/logs/tet_vm_setup.log` pour connaître la raison de l'échec du déploiement des conteneurs d'agents SPAN.

Tout autre problème d'enregistrement ou de connectivité des agents peut être résolu de la même manière que pour les agents exécutés sur un hôte, à l'aide de la commande *docker exec* :

- `docker exec <cid> ps -ef` signale les deux instances `tet-engine, tet-engine check_conf` et deux instances `/usr/local/tet/tet-sensor -f /usr/local/tet/conf/.sensor_config`, une avec l'utilisateur racine et une avec l'utilisateur tet -sensor, ainsi que l'instance gestionnaire de processus `/usr/bin/ python /usr/bin/supervisord -c /etc/supervisord.conf -n`.
- `docker exec <cid> cat /usr/local/tet/log/tet-sensor.log` affiche les journaux de l'agent;
- `docker exec <cid> cat /usr/local/tet/log/fetch_sensor_id.log` affiche les journaux des enregistrements de l'agent;
- `docker exec <cid> cat /usr/local/tet/log/check_conf_update.log` affiche les journaux d'interrogation de la mise à jour de la configuration;

  Si nécessaire, le trafic vers/depuis le conteneur peut être surveillé à l'aide de la commande tcpdump après avoir été défini dans l'espace de nom réseau du conteneur :

  1. Récupérez l'espace de noms réseau du conteneur (SandboxKey) à l'aide de docker inspect <cid> | grep SandboxKey;
  2. Inscrit dans l'espace de noms du réseau du conteneur nsenter --net=/var/run/docker/netns/...;
  3. Surveillez le trafic tcpdump -i eth0 -n.

Limites

Unité	Limite
Nombre maximal de connecteurs ERSPAN sur un appareil d'acquisition (ingest appliance) Cisco Secure Workload	3

Unité	Limite
Nombre maximal de connecteurs ERSPAN sur un détenteur (portée racine)	24 (12 pour TaaS)
Nombre maximal de connecteurs ERSPAN sur Cisco Secure Workload	450

Connecteurs pour points terminaux

Les connecteurs pour points terminaux fournissent un contexte de point terminal pour Cisco Secure Workload.

Connecteur	Description	Déployé sur une appliance virtuelle
AnyConnect	Recueillez des données de télémétrie à partir du module de visibilité réseau (Network Visibility Module ou NVM) Cisco AnyConnect et enrichissez les inventaires de points terminaux avec les attributs des utilisateurs.	Acquisition de Cisco Secure Workload
ISE	Recueillez des renseignements sur les points terminaux et les inventaires gérés par les appareils Cisco ISE et enrichissez les inventaires des points terminaux avec des attributs utilisateur et des étiquettes de groupe sécurisées (SGL).	Cisco Secure Workload Edge

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

AnyConnect Connector

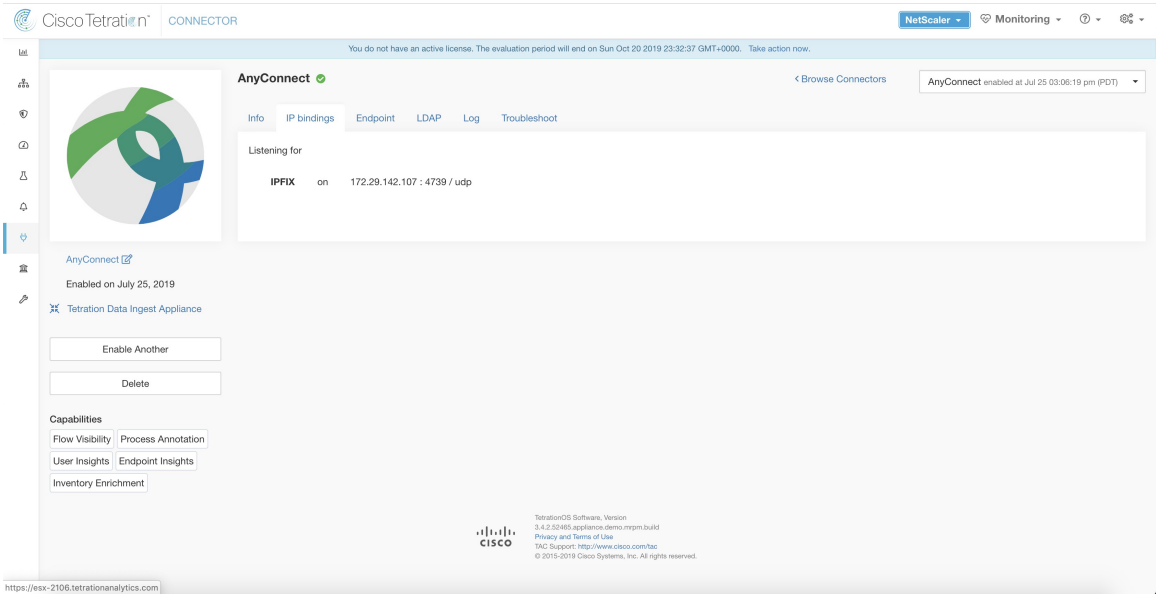
AnyConnect connector monitors endpoints that run Cisco AnyConnect Secure Mobility Client with Network Visibility Module (NVM). Using this solution, the hosts do not need to run any software agents on endpoints, because NVM sends host, interface, and flow records in IPFIX format to a collector (e.g., AnyConnect connector).

AnyConnect connector does the following high-level functions.

1. Register each endpoint (supported user devices such as a desktop, a laptop, or a smartphone) on Cisco Cisco Secure Workload as an AnyConnect agent.
2. Update interface snapshots from these endpoints with Secure Workload.
3. Send flow information exported by these endpoints to Cisco Secure Workload collectors.
4. Periodically send process snapshots for processes that generate flows on the endpoints tracked by the AnyConnect connector.

5. Label endpoint interface IP addresses with Lightweight Directory Access Protocol (LDAP) attributes corresponding to the logged-in-user at each endpoint.

Figure 11: AnyConnect connector



Qu'est-ce qu'AnyConnect NVM?

AnyConnect NVM offre une visibilité et une surveillance du comportement des terminaux et des utilisateurs sur site et hors site. Il recueille des informations à partir des points terminaux qui incluent le contexte suivant.

1. **Contexte d'appareil/point terminal** : informations spécifiques à l'appareil ou au point terminal.
2. **Contexte utilisateur** : utilisateurs associés au flux.
3. **Contexte d'application** : processus associés au flux.
4. **Contexte de l'emplacement** : attributs propres à l'emplacement, si disponibles.
5. **Contexte de destination** : nom de domaine complet (FQDN) de la destination. AnyConnect NVM génère trois types d'enregistrements.

Enregistrement NVM	Description
Enregistrement de point terminal	Informations sur le périphérique ou le point terminal, y compris l'identifiant unique de périphérique (UDID), le nom d'hôte, le nom du système d'exploitation, la version du système d'exploitation et le fabricant.
Enregistrement d'interface	Informations sur chaque interface du point terminal, y compris l'UDID du point terminal, l'identifiant unique de l'interface (UID), l'indice d'interface, le type d'interface, le nom de l'interface et l'adresse MAC.

Enregistrement NVM	Description
Enregistrement de flux	Renseignements sur les flux observés sur le point terminal, y compris l'UDID du point terminal, l'UID de l'interface, le 5-tuple (source/destination ip/port et protocole), le nombre d'octets entrants/sortants, les renseignements sur le processus, les renseignements sur l'utilisateur et le nom de domaine complet de la destination.

Chaque enregistrement est généré et exporté au format de protocole IPFIX. Lorsque le périphérique se trouve dans un réseau de confiance (sur site/VPN), AnyConnect NVM exporte les enregistrements vers un collecteur configuré. Le connecteur AnyConnect est un exemple de collecteur IPFIX qui peut recevoir et traiter le flux IPFIX de AnyConnect NVM.

Note Le connecteur AnyConnect prend en charge AnyConnect NVM à partir des versions 4.2 et ultérieures de Cisco AnyConnect Secure Mobility Client.

How to configure AnyConnect NVM

See How to Implement AnyConnect NVM document for step by step instructions on how to implement AnyConnect NVM using either Cisco Secure Firewall ASA or Cisco Identity Services engine (ISE). Once NVM module is deployed, an NVM profile should be specified and pushed to and installed on the endpoints running Cisco AnyConnect Secure Mobility Client. When specifying NVM profile, the IPFIX collector should be configured to point to AnyConnect connector on port 4739.

AnyConnect connector also registers with Cisco Secure Workload as a Cisco Secure Workload AnyConnect Proxy agent.

Traitement des enregistrements NVM

Le connecteur AnyConnect traite les enregistrements NVM AnyConnect comme indiqué ci-dessous.

Enregistrement de point terminal

Lors de la réception d'un enregistrement de point terminal, le connecteur AnyConnect enregistre ce point terminal en tant qu'agent AnyConnect sur la charge de travail sécurisée. Le connecteur AnyConnect utilise les renseignements spécifiques au point terminal présents dans l'enregistrement NVM avec le certificat du connecteur AnyConnect pour enregistrer le point terminal. Une fois qu'un point terminal est enregistré, le plan de données du point terminal est activé en créant une nouvelle connexion à l'un des collecteurs dans Cisco Secure Workload. En fonction de l'activité (enregistrements de flux) de ce point terminal, le connecteur AnyConnect connecte l'agent AnyConnect correspondant à ce point à la grappe périodiquement (20 à 30 minutes).

AnyConnect NVM commence à diffuser la version de l'agent à partir de la version 4.9. Par défaut, le point terminal AnyConnect est enregistré en tant que version 4.2.x sur Cisco Secure Workload. Cette version indique la version minimale NVM AnyConnect prise en charge. Pour les points terminaux AnyConnect dotés dans la version 4.9 ou ultérieure, l'agent AnyConnect correspondant sur Cisco Secure Workload affichera la version réelle installée.

Note La version installée de l'agent AnyConnect n'est pas contrôlée par Cisco Secure Workload. La tentative de mise à niveau de l'agent terminal AnyConnect sur l'interface utilisateur Cisco Secure Workload n'a pas d'effet.

Enregistrement d'interface

L'adresse IP de l'enregistrement d'interface pour une interface donnée ne fait pas partie de l'enregistrement d'interface NVM AnyConnect. L'adresse IP d'une interface est déterminée lorsque les enregistrements de flux commencent à être envoyés à partir du point terminal pour cette interface. Une fois que l'adresse IP est déterminée pour une interface, le connecteur AnyConnect envoie un instantané complet de toutes les interfaces de ce point terminal dont l'adresse IP est déterminée au serveur de configuration de Cisco Secure Workload. Le VRF est ainsi associé aux données de l'interface et les flux arrivant sur ces interfaces seront désormais marqués par ce VRF.

Enregistrement de flux

Lors de la réception d'un enregistrement de flux, le connecteur AnyConnect le traduit au format que Cisco Secure Workload comprend et envoie FlowInfo sur le plan de données correspondant à ce point terminal. En outre, il stocke localement les informations de processus incluses dans l'enregistrement de flux. De plus, si une configuration LDAP est fournie au connecteur AnyConnect, celui-ci détermine les valeurs des attributs LDAP configurés de l'utilisateur connecté du point terminal. Les attributs sont associés à l'adresse IP du point terminal où le flux s'est produit. Périodiquement, les informations sur les processus et les étiquettes des utilisateurs sont transmises à Cisco Secure Workload.

Note Chaque connecteur AnyConnect ne signalera que les points terminaux, les interfaces et les flux pour un VRF. Les points terminaux et les interfaces signalés par le connecteur AnyConnect sont associés au VRF en fonction de la configuration du VRF de l'agent dans Cisco Secure Workload. Les flux exportés par l'agent de connecteur AnyConnect au nom du point terminal AnyConnect appartiennent au même VRF. Pour configurer le VRF pour l'agent, accédez à : **Manage (Gestion)** > **Agents (Agents)** puis cliquez sur l'onglet **Configuration**. Dans cette page, dans la section « Agent Remote VRF Configurations » (configurations de VRF à distance de l'agent), cliquez sur « Create Config » (Créer une configuration) et fournissez les détails du connecteur AnyConnect. Le formulaire demande à l'utilisateur de fournir le nom du VRF, le sous-réseau IP de l'hôte sur lequel l'agent est installé, et la plage de numéros de ports qui peuvent potentiellement envoyer des enregistrements de flux à la grappe.

UDID en double dans les points terminaux Windows

Si des machines de point terminal sont clonées à partir de la même image d'or, il est possible que les UDID de tous les points terminaux clonés soient identiques. Dans ce cas, le connecteur AnyConnect reçoit les enregistrements de point terminal de ces points terminaux avec le même UDID et les enregistre sur Cisco Secure Workload avec le même UDID. Lorsque des enregistrements d'interface ou de flux sont reçus par le connecteur de ces points terminaux, le connecteur ne peut pas déterminer l'agent AnyConnect correct sur Cisco Secure Workload auquel associer les données. Le connecteur associe toutes les données à un seul point terminal (et il n'est pas déterministe).

Pour résoudre ce problème, la version 4.8 d'AnyConnect NVM est livrée avec un outil appelé *dartcli.exe* pour déterminer et régénérer l'UDID sur le point terminal.

- *dartcli.exe -u* récupère l'UDID du point terminal.
- *dartcli.exe -nu* régénère l'UDID du point terminal. Pour exécuter cet outil, procédez comme suit :

```
    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 8D0D1E8FA0AB09BE82599F10068593E41EF1BFFF

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-nu
    Are you sure you want to re-generate UDID [y/n]: y
    Adding nonce success
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5
```

Tâches périodiques

Périodiquement, le connecteur AnyConnect envoie des instantanés de processus et des étiquettes d'utilisateur sur les inventaires de points terminaux AnyConnect.

1. **Instantanés de processus** : toutes les 5 minutes, le connecteur AnyConnect parcoure les processus qu'il gère localement pendant cet intervalle et envoie un instantané de processus pour tous les points terminaux qui ont reçu des flux pendant cet intervalle.
2. **Étiquettes utilisateur** : toutes les 2 minutes, le connecteur AnyConnect parcourt les étiquettes utilisateur LDAP qu'il gère localement et met à jour les étiquettes utilisateur sur ces adresses IP.

Pour les étiquettes d'utilisateur, le connecteur AnyConnect crée un instantané local des attributs LDAP de tous les utilisateurs de l'organisation. Lorsque le connecteur AnyConnect est activé, la configuration LDAP (informations sur le serveur/port, attributs à récupérer pour un utilisateur, attribut qui contient le nom d'utilisateur) peut être fournie. De plus, les renseignements d'authentification de l'utilisateur LDAP pour accéder au serveur LDAP peuvent être fournis. Les renseignements d'authentification des utilisateurs LDAP sont chiffrés et ne sont jamais révélés dans le connecteur AnyConnect. Si vous le souhaitez, un certificat LDAP peut être fourni pour un accès sécurisé au serveur LDAP.

Note Le connecteur AnyConnect crée un nouvel instantané LDAP local toutes les 24 heures. Cet intervalle est configurable dans la configuration LDAP du connecteur.

Comment configurer le connecteur

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *LDAP* : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour choisir l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Point terminal* : pour en savoir plus, consultez Configuration du point terminal.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

De plus, les ports d'écoute du protocole IPFIX sur le connecteur peuvent être mis à jour sur le conteneur Docker dans l'appareil d'acquisition Cisco Secure Workload à l'aide d'une commande autorisée. Cette commande peut être exécutée sur l'appareil en fournissant l'ID du connecteur, le type de port à mettre à jour et les renseignements sur le nouveau port. L'ID du connecteur se trouve sur la page du connecteur dans l'interface utilisateur Cisco Secure Workload. Pour plus d'informations, consultez l'article mise à jour-écoute-ports.

Limites

Unité	Limite
Nombre maximal de connecteurs AnyConnect sur un appareil d'acquisition Cisco Secure Workload	1
Nombre maximal de connecteurs AnyConnect sur un détenteur (portée racine)	50
Nombre maximal de connecteurs AnyConnect sur Cisco Secure Workload	500

ISE Connector

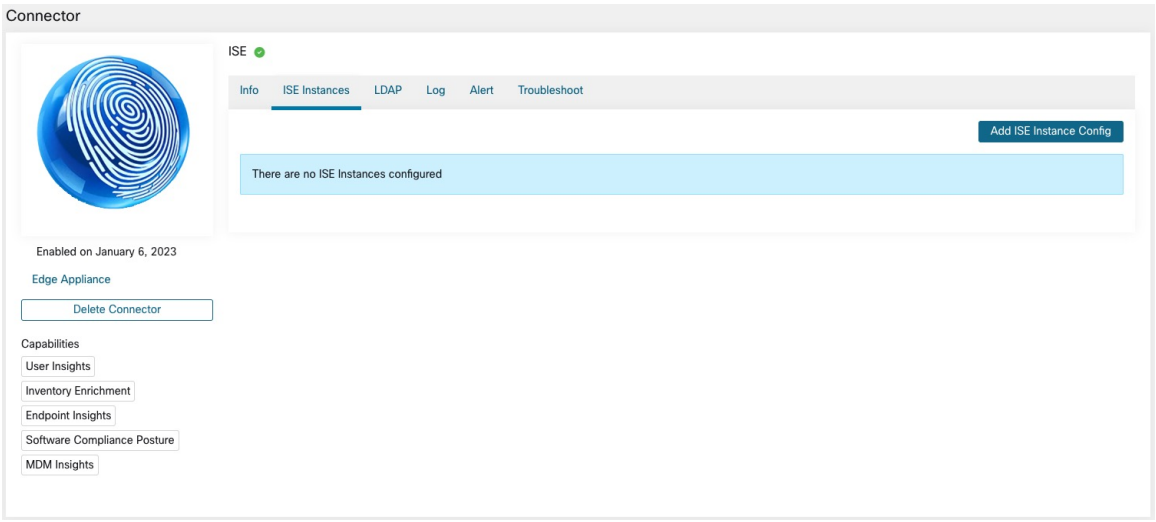
ISE connector in Secure Workload connects with Cisco Identity Services Engine (ISE), using Cisco Platform Exchange Grid (pxGrid), to retrieve contextual information about endpoints reported by ISE. Using these solutions, we can obtain enriched metadata for endpoints.

The ISE connector in Secure Workload connects with Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (ISE-PIC) using the Cisco Platform Exchange Grid (pxGrid), to retrieve contextual information, such as metadata, for endpoints reported by ISE.

An ISE connector performs these functions:

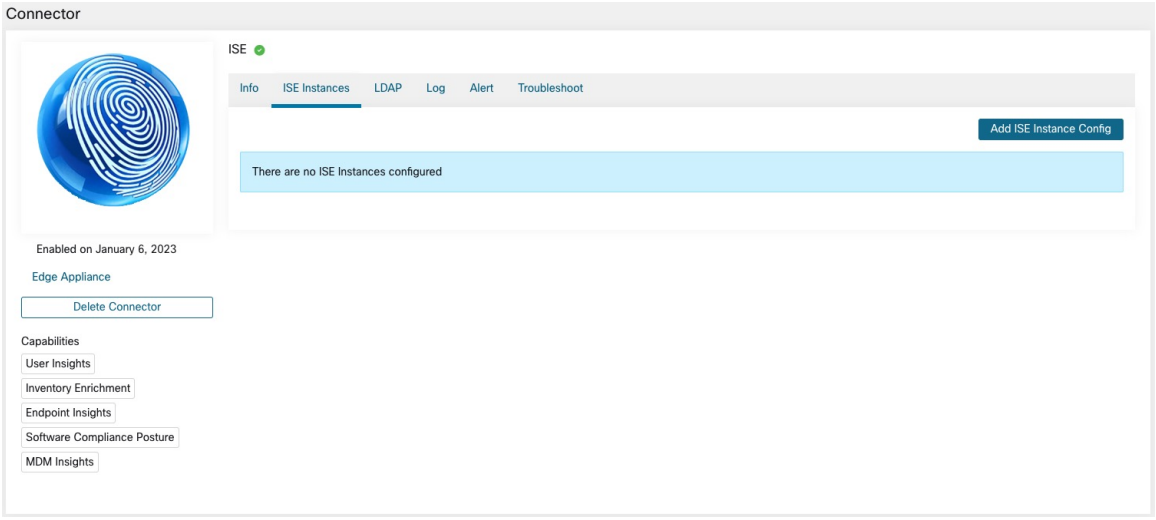
1. Register each endpoint viewed by ISE on Cisco Secure Workload as an ISE endpoint agent.
2. Update metadata information regarding these endpoints to Cisco Secure Workload including MDM details, authentication, Security Group labels, and others.
3. Periodically take a snapshot and update cluster with active endpoints visible on ISE.

Figure 12: ISE connector



1. Registers each endpoint that are identified as an ISE endpoint on Secure Workload.
2. Updates metadata information on Secure Workload regarding the endpoints, such as MDM details, authentication, Security Group labels, ISE group name, and ISE group type.
3. Periodically takes a snapshot and updates the cluster with active endpoints visible on the ISE.

Figure 13: ISE connector



Note Each ISE connector will register only endpoints and interfaces for one VRF. The endpoints and interfaces reported by ISE connector are associated with the VRF based on the Agent VRF configuration in Secure Workload. To configure the VRF for the agent, go to: **Manage** > **Agents** and click the **Configuration** tab. In this page, under the **Agent Remote VRF Configurations** section, click **Create Config** and provide the details about the ISE connector. The form requests the user to provide: the name of the VRF, IP subnet of the host on which the agent is installed, and range of port numbers that can potentially register ISE endpoints and interfaces on Secure Workload.

Note The ISE endpoint agents are not listed on the Agents List page; instead ISE endpoints with the attributes can be viewed on the Inventory page.

Comment configurer le connecteur

Note ISE version 2.4+ et ISE PIC version 3.1+ sont nécessaires pour cette intégration.

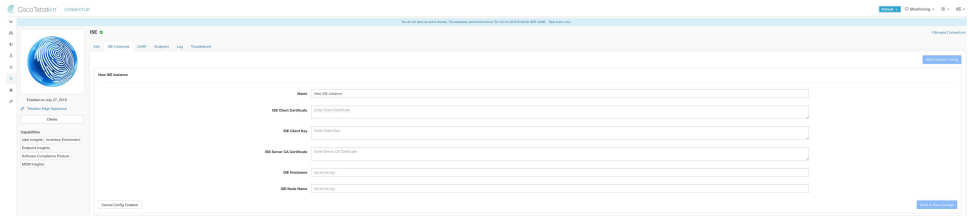
Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Pour les connecteurs ISE, les adresses IPv4 et IPv6 (mode double pile) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Les configurations suivantes sont autorisées sur le connecteur.

- *Instance ISE* : le connecteur ISE peut se connecter à plusieurs instances ISE en utilisant les configurations fournies. Chaque instance nécessite des renseignements d'authentification de certificat ISE ainsi qu'un nom d'hôte et un nom de nœud pour se connecter à ISE. Pour en savoir plus, consultez Configuration de l'instance ISE.
- *LDAP* : la configuration LDAP prend en charge la découverte des attributs LDAP et fournit un flux de travail pour sélectionner l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à récupérer pour chaque utilisateur. Pour en savoir plus, consultez la section Découverte.
- *Point terminal* : pour en savoir plus, consultez Configuration du point terminal.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration du point terminal.

Configuration de l'instance ISE

Figure 14: Configuration d'instance ISE



Note À partir de la version 3.7 de Cisco Secure Workload, le certificat SSL pour le nœud pxGrid de Cisco ISE nécessite d'autres noms de sujet (SAN) pour cette intégration. Assurez-vous que la configuration de certification des nœuds ISE est effectuée par votre administrateur ISE avant de procéder à l'intégration avec Cisco Secure Workload.

Pour vérifier le certificat de votre nœud pxGrid et confirmer si le SAN est configuré, vous devez procéder comme suit pour vérifier le certificat d'ISE.

Procedure

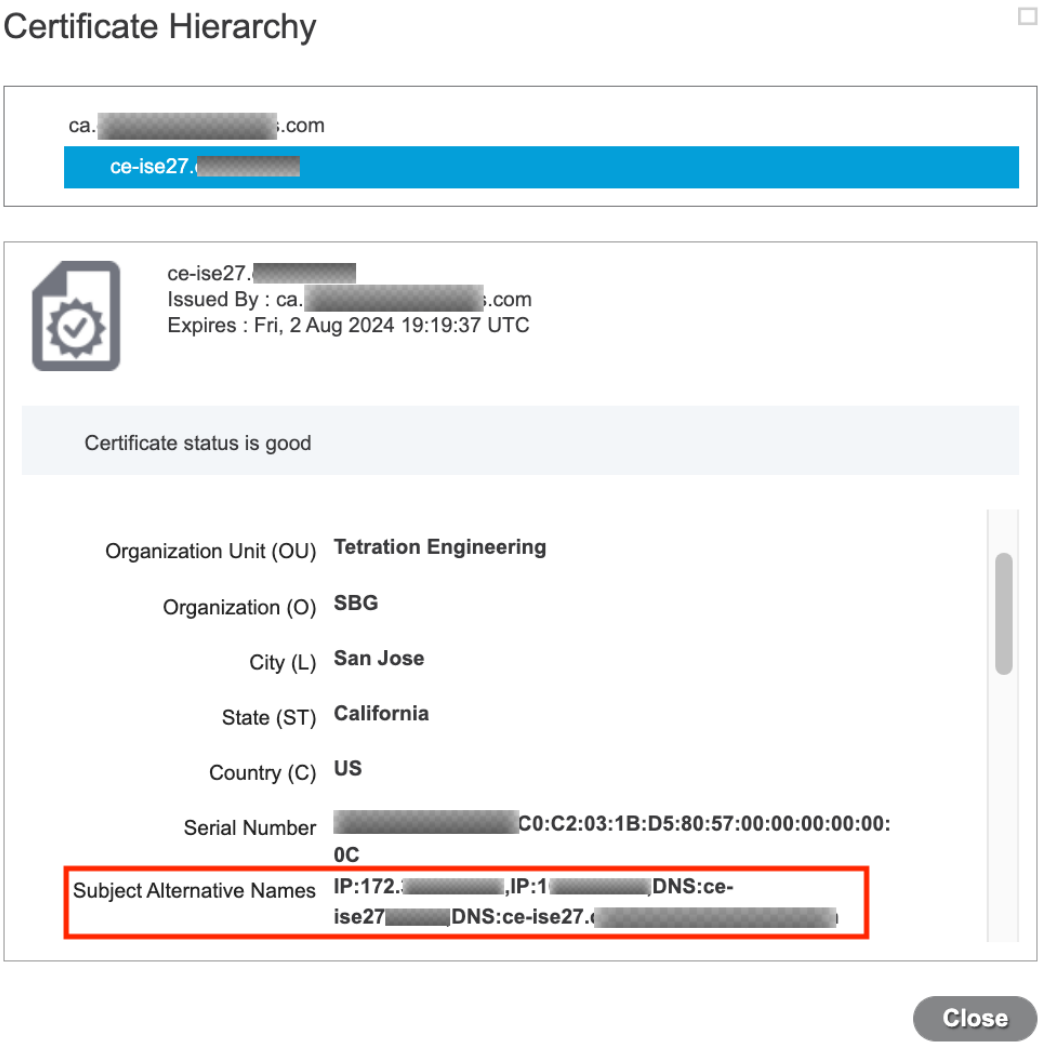
Étape 1 Rendez-vous à **Certificates** (Certificats) sous **Administration** > **System** (Système).

Étape 2 Sous **Certificate Management** (Gestion du certificat) , sélectionnez **System Certificates** (Certificat système), sélectionnez votre certificat pxGrid « utilisé par » et choisissez **View** (afficher) pour examiner le certificat de nœud pxGrid.

Étape 3 Faites défiler le certificat et vérifiez que les Subject Alternative Names (autres noms de sujet) sont configurés pour ce certificat.

Étape 4 Ce certificat doit être signé par une autorité de certification (CA) valide, qui doit également être utilisée pour signer le certificat client pxGrid utilisé par le connecteur Cisco Secure Workload ISE.

Figure 15: Exemple de certificat de nœud ISE valide



Étape 5 Vous pouvez maintenant générer la demande de signature de certificat client pxGrid en utilisant le modèle suivant sur n'importe quel hôte installé avec OpenSSL.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = YOUR_COUNTRY
ST = YOUR_STATE
L = YOUR_CITY
O = YOUR_ORGANIZATION
OU = YOUR_ORGANIZATION_UNIT
CN = ise-connector.example.com
[v3_req]
subjectKeyIdentifier = hash
```

```
basicConstraints = critical,CA:false
subjectAltName = @alt_names
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = serverAuth,clientAuth
[alt_names]
IP.1 = 10.x.x.x
DNS.1 = ise-connector.example.com
```

Enregistrez le fichier sous le nom « example-connector.cfg » et utilisez la commande OpenSSL de votre hôte pour générer une requête de signature de certificat (CSR) et la clé privée du certificat à l'aide de la commande suivante.

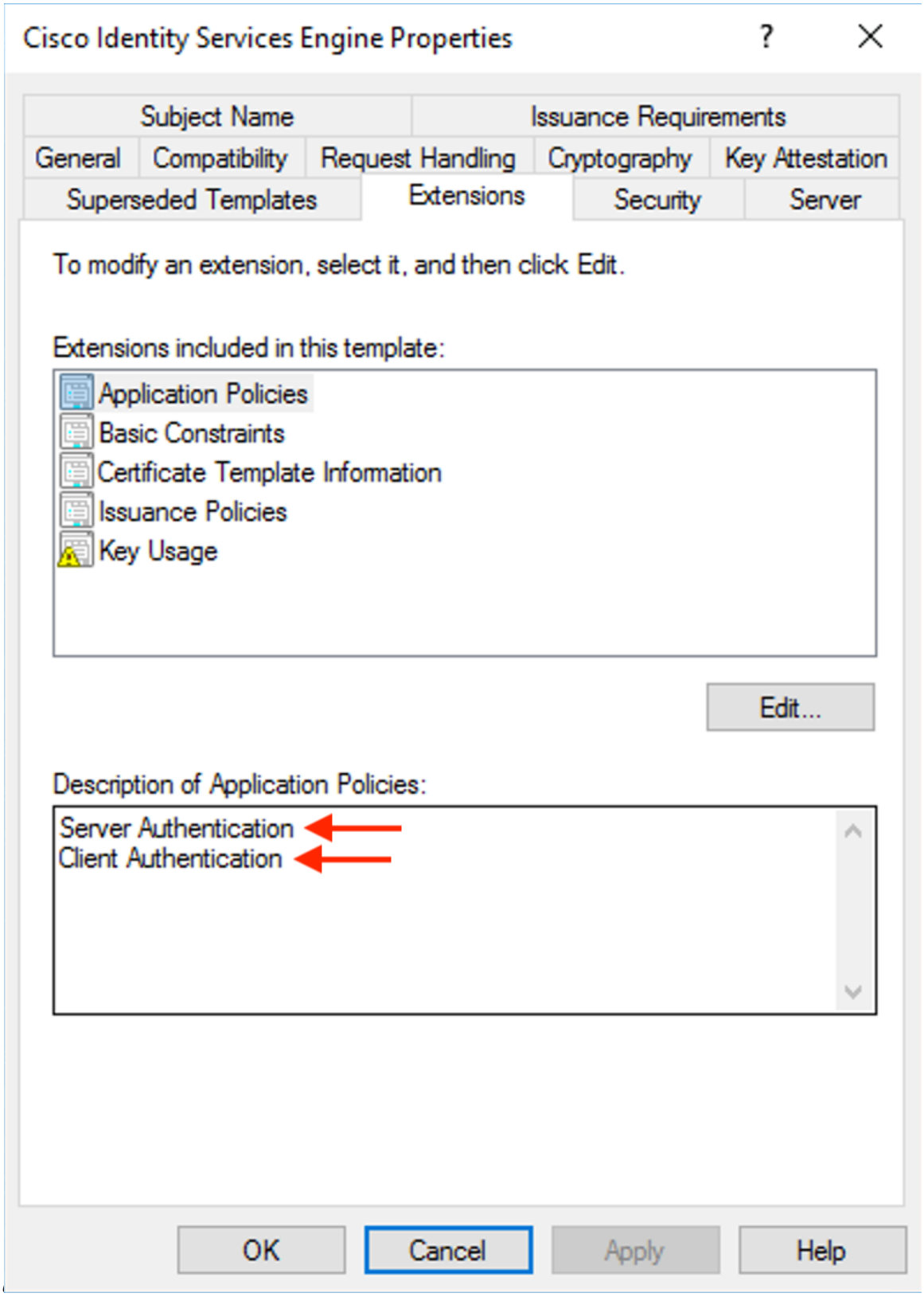
```
openssl req -newkey rsa:2048 -keyout example-connector.key -nodes -out example-connector.csr
 -config example-connector.cfg
```

Étape 6 Signez la requête de signature de certificat (CSR) de votre autorité de certification en utilisant un serveur d'autorité de certification Windows. Si vous utilisez également un serveur d'autorité de certification Windows, exécutez la commande suivante pour signer la CSR du client pxGrid.

```
certreq -submit -binary -attrib "CertificateTemplate:CiscoIdentityServicesEngine"
example-connector.csr example-connector.cer
```

Note L'autorité de certification Windows nécessite un modèle de certificat. Ce modèle doit contenir les extensions suivantes.

Figure 16: Extensions des politiques d'application pour un modèle de



Étape 7 Copiez le certificat client signé et l'autorité de certification racine au format PEM sur votre hôte. Il s'agit du même hôte qui génère la demande de signature de certificat (CSR) du client et la clé privée. Utilisez OpenSSL pour vous assurer que le certificat client est au format PEM X.509. Exécutez la commande suivante à l'aide d'OpenSSL pour convertir le certificat client signé au format PEM X.509.

```
openssl x509 -inform der -in example-connector.cer -out example-connector.pem
```

Étape 8 Vous pouvez également confirmer le PEM signé par l'autorité de certification en utilisant la commande suivante.

```
openssl verify -CAfile root-ca.example.com.pem example-connector.pem
example-connector.pem: OK
```

Note Pour le déploiement à nœuds multiples d'ISE avec pxGrid, tous les nœuds pxGrid doivent faire confiance aux certificats utilisés pour le connecteur Cisco Secure Workload ISE.

Étape 9 En utilisant les noms de fichiers de l'exemple ci-dessus, copiez le certificat client ISE - example-connector.pem, la clé du client - example-connector.key et l'autorité de certification – root-ca.example.com.pem dans les champs respectifs de la page de configuration ISE sur Cisco Secure Workload comme indiqué ci-dessous.

Note Avant de mettre à niveau vers la dernière version de Cisco Secure Workload, veillez à supprimer le connecteur ISE pour supprimer toutes les données de configuration existantes. Une fois la mise à niveau terminée, configurez le connecteur ISE avec les nouveaux filtres que vous souhaitez appliquer.

Figure 17: Configuration du connecteur ISE

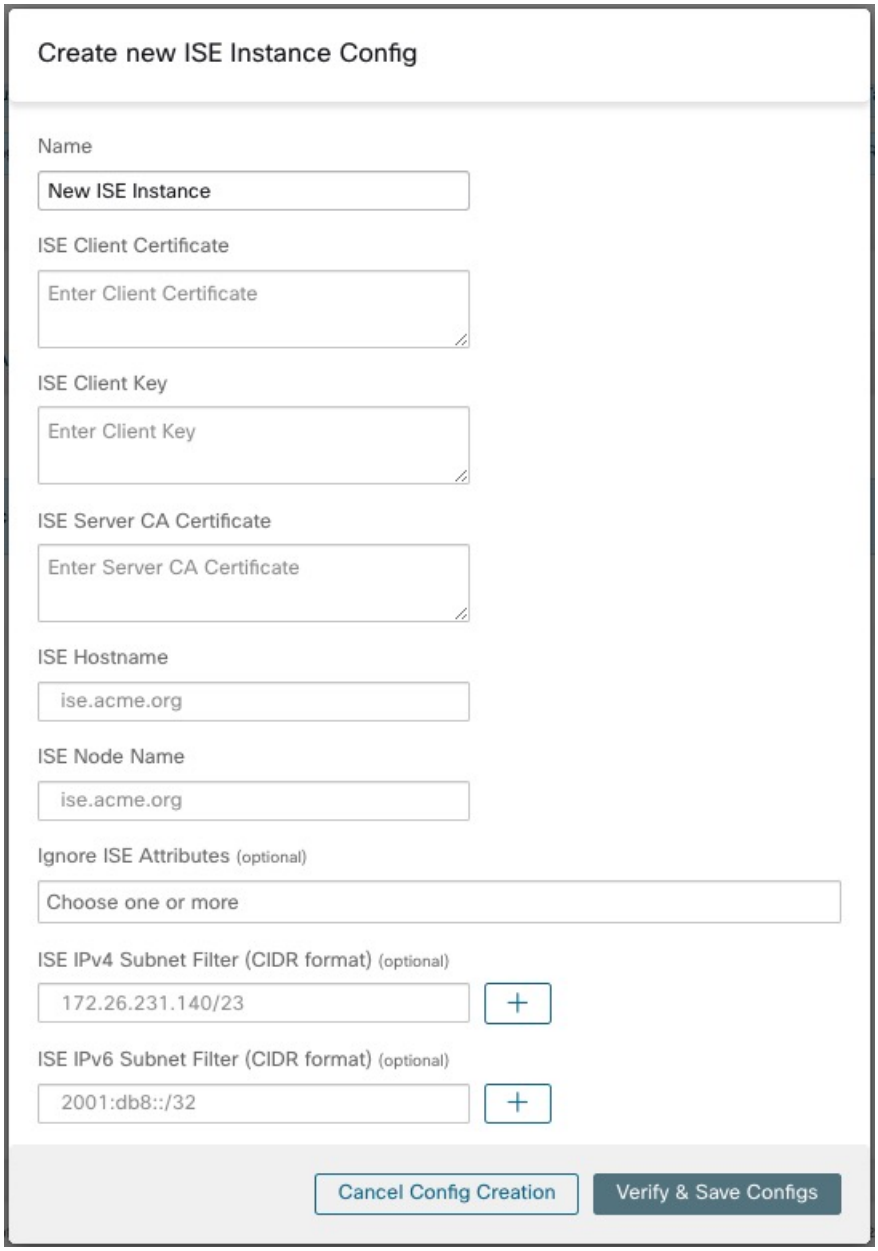


Table 2: Configuration du connecteur ISE

Champ	Description
Nom	Saisissez un nom d'instance ISE.
Certificat client ISE	Copiez et collez le certificat client ISE.

Champ	Description
Clé de client ISE	Copiez et collez la clé client ISE. La clé client doit être une clé en clair, qui n'est pas protégée par un mot de passe.
Certificat de l'autorité de certification du serveur ISE	Copiez et collez le certificat de l'autorité de certification racine.
Nom d'hôte ISE	Saisissez le nom d'hôte ISE (nom de domaine complet).
Nom de nœud ISE	Saisissez un nom de nœud
Ignorer les attributs ISE (facultatif)	Sélectionnez un ou plusieurs attributs ISE dans la liste. Utilisez cette option si vous ne souhaitez pas intégrer toutes les informations contextuelles des points terminaux signalés par le biais d'ISE.
Filtre de sous-réseau IPv4 ISE (format CIDR) (facultatif)	Saisissez plusieurs sous-réseaux IPv4 pour filtrer les points terminaux ISE.
Filtre de sous-réseau IPv6 ISE (format CIDR) (facultatif)	Saisissez plusieurs sous-réseaux IPv6 pour filtrer les points terminaux ISE.

Note

- Si une adresse IP est utilisée au lieu d'un nom de domaine complet pour le nom d'hôte ISE, utilisez l'adresse IP dans le SAN du certificat de l'autorité de certification ISE, sinon des échecs de connexion pourraient se produire.
- Le nombre de points terminaux actifs sur ISE n'est pas un instantané, il dépend des configurations sur ISE et de la durée d'agrégation pour le calcul de la mesure. Le nombre d'agents sur Cisco Secure Workload est toujours un instantané basé sur la dernière récupération de mises à jour d'ISE et de pxgrid, généralement le nombre de périphériques actifs au cours de la dernière journée (la fréquence d'actualisation par défaut des instantanés complets est d'un jour). En raison de la différence dans la façon dont ces nombres sont représentés, il est possible qu'ils ne correspondent pas toujours.

Traitement des enregistrements ISE

Le connecteur ISE traite les enregistrements comme décrit ci-dessous.

Enregistrement de point terminal

Le connecteur ISE se connecte à l'instance ISE et s'abonne à toutes les mises à jour des points terminaux sur pxGrid. Lors de la réception d'un enregistrement de point terminal, le connecteur ISE enregistre ce point terminal en tant qu'agent ISE sur Cisco Secure Workload. Le connecteur ISE utilise les informations spécifiques au point terminal présentes dans l'enregistrement de ce dernier ainsi que le certificat du connecteur ISE pour enregistrer le point terminal. Une fois qu'un point terminal est enregistré. Le connecteur ISE utilise l'objet de point terminal pour l'enrichissement de l'inventaire en l'envoyant en tant qu'étiquettes d'utilisateur sur

Cisco Secure Workload. Lorsque le connecteur ISE reçoit un point terminal déconnecté d'ISE, il supprime l'enrichissement d'inventaire de Cisco Secure Workload.

Enregistrement de groupe de sécurité

ISE connect s'abonne également aux mises à jour sur les modifications des étiquettes de groupes de sécurité via pxGrid. Lors de la réception de cet enregistrement, les connecteurs ISE conservent une base de données locale. ISE utilise cette base de données pour mapper le nom SGT avec la valeur lors de la réception d'un enregistrement de point terminal.

Tâches périodiques

Le connecteur ISE partage régulièrement des étiquettes d'utilisateur sur les inventaires de points terminaux ISE.

1. **instantanés de points terminaux** : toutes les 20 heures, le connecteur ISE récupère un instantané des points terminaux et des étiquettes de groupes de sécurité de l'instance ISE et met à jour la grappe si des modifications sont détectées. Cet appel ne tient pas compte des points terminaux déconnectés au cas où nous ne verrions pas de points terminaux sur Cisco Secure Workload en provenance d'ISE.
2. **Étiquettes d'utilisateur** : toutes les deux minutes, le connecteur ISE balaye les étiquettes d'utilisateur LDAP et de point terminal ISE gérées localement et met à jour les étiquettes d'utilisateur sur ces adresses IP.

Pour les étiquettes d'utilisateur, le connecteur ISE crée un instantané local des attributs LDAP de tous les utilisateurs de l'organisation. Lorsque le connecteur ISE est activé, la configuration LDAP (informations sur le serveur/port, attributs à récupérer pour un utilisateur, attribut qui contient le nom d'utilisateur) peut être fournie. De plus, les renseignements d'authentification de l'utilisateur LDAP pour accéder au serveur LDAP peuvent être fournis. Les informations d'authentification des utilisateurs LDAP sont chiffrées et ne sont jamais révélées dans le connecteur ISE. Si vous le souhaitez, un certificat LDAP peut être fourni pour un accès sécurisé au serveur LDAP.

Note Le connecteur ISE crée un nouvel instantané LDAP local toutes les 24 heures. Cet intervalle est configurable dans la configuration LDAP du connecteur.

Note Lors de la mise à niveau d'un périphérique Cisco ISE, le connecteur ISE devra être reconfiguré avec les nouveaux certificats générés par ISE après la mise à niveau.

Limites

Unité	Limite
Nombre maximal d'instances ISE qui peuvent être configurées sur un connecteur ISE	20
Nombre maximal de connecteurs ISE sur un appareil de périphérieCisco Secure Workload	1
Nombre maximal de connecteurs ISE sur un détenteur (portée racine)	1

Unité	Limite
Nombre maximal de connecteurs ISE sur Cisco Secure Workload	150

Connecteurs pour l'enrichissement de l'inventaire

Les connecteurs pour l'enrichissement de l'inventaire fournissent des métadonnées et du contexte supplémentaires sur les inventaires (adresses IP) surveillés par Cisco Secure Workload.

Connecteur	Description	Déployé sur une appliance virtuelle
ServiceNow	Recueillez des renseignements sur le point terminal de l'instance ServiceNow et enrichissez l'inventaire avec les attributs ServiceNow	Cisco Secure Workload Edge
Consultez aussi :	connecteurs infonuagiques	–

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs.

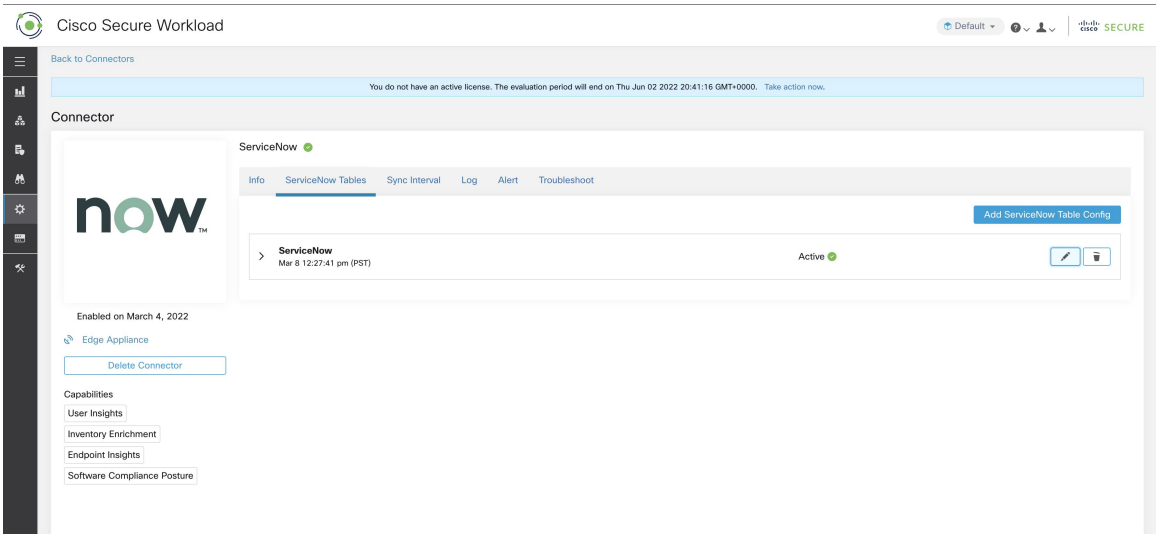
Connecteur ServiceNow

Le connecteur ServiceNow se connecte à l'instance ServiceNow pour obtenir toutes les étiquettes liées à la CMDB ServiceNow pour les points terminaux de l'inventaire ServiceNow. En utilisant cette solution, nous pouvons obtenir des métadonnées améliorées pour les points terminaux dans Cisco Secure Workload.

Le connecteur ServiceNow effectue les fonctions principales suivantes.

1. Mettre à jour les métadonnées ServiceNow dans l'inventaire de Cisco Secure Workload pour ces points terminaux.
2. Prendre régulièrement des instantanés et mettre à jour les étiquettes sur ces points terminaux.

Figure 18: Connecteur ServiceNow



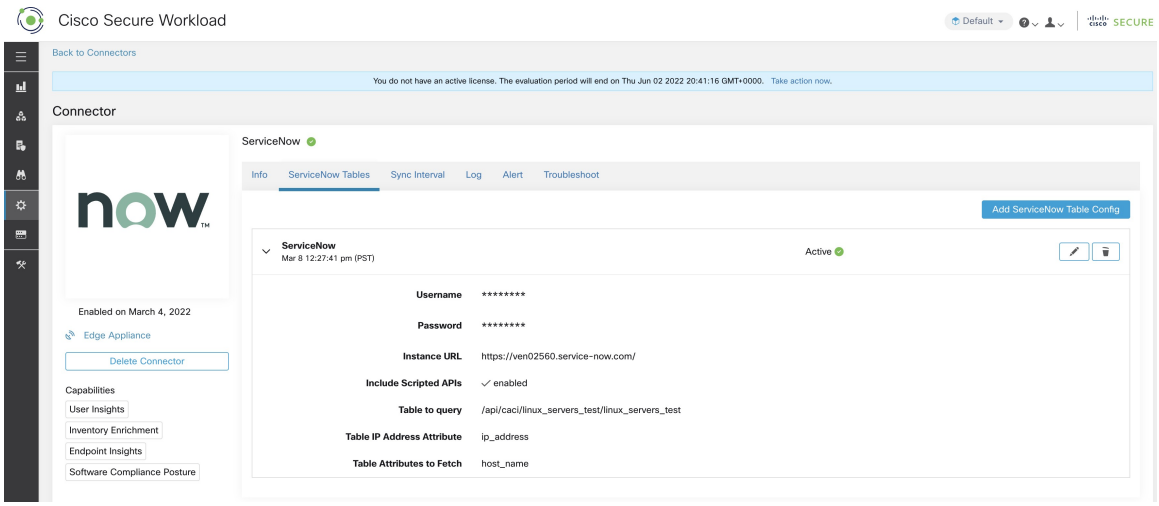
Comment configurer le connecteur ServiceNow

Pour en savoir plus sur les appliances virtuelles requises, consultez Appliances virtuelles pour les connecteurs. Les configurations suivantes sont autorisées sur le connecteur.

- *ServiceNow Tables* : la fonction ServiceNow Tables configure l'instance ServiceNow avec ses informations d'authentification et les informations sur les tables ServiceNow dans lesquelles récupérer les données.
- *API REST scriptée* : les tableaux de l' API REST scriptée ServiceNow peuvent être configurés de la même manière que les tableaux ServiceNow.
- *Sync Interval* : la configuration de l'intervalle de synchronisation permet de modifier la fréquence à laquelle Cisco Secure Workload doit interroger l'instance de ServiceNow pour obtenir des données mises à jour.
- *Log* (Journal) : pour en savoir plus, consultez la Configuration de la journalisation.

Configuration de l'instance ServiceNow

Figure 19: Configuration de l'instance ServiceNow



Vous aurez besoin des éléments suivants pour configurer avec succès une instance ServiceNow.

1. Nom d'utilisateur ServiceNow
2. Mot de passe ServiceNow
3. URL de l'instance ServiceNow
4. Inclure les API scriptées

Par la suite, Cisco Secure Workload effectue une découverte de tous les tableaux à partir de l'instance ServiceNow et des API REST scriptées (uniquement si la case Include Scripted APIs (Inclure les API scriptées) est cochée). Il présente à l'utilisateur la liste des tableaux parmi lesquels choisir. Une fois qu'un utilisateur a sélectionné un tableau, Cisco Secure Workload récupère toute la liste des attributs de ce tableau pour que l'utilisateur puisse les sélectionner. L'utilisateur doit choisir l'attribut ip_address dans le tableau comme clé. Ensuite, l'utilisateur peut choisir jusqu'à 10 attributs uniques dans le tableau. Consultez les figures suivantes pour chaque étape.

Note Le connecteur ServiceNow peut uniquement prendre en charge l'intégration avec des tableaux comportant un champ d'**adresse IP**.

Note Pour intégrer les API REST scriptées de ServiceNow, vous devez cocher la case API scriptées, ce qui vous donnerait un flux de travail similaire à tout autre tableau.

Note Pour que les API REST scriptées s'intègrent au connecteur ServiceNow, elles ne peuvent pas avoir de paramètres de chemin. En outre, elles doivent prendre en charge **sysparm_limit,sysparm_fields and sysparm_offset** en tant que paramètres de requête.

Note Les rôles d'utilisateur ServiceNow doivent inclure **cmdb_read** pour les tableaux et **web_service_admin** pour les API REST scriptées afin de s'intégrer à Cisco Cisco Secure Workload.

Figure 20: Première étape de la configuration de l'instance ServiceNow

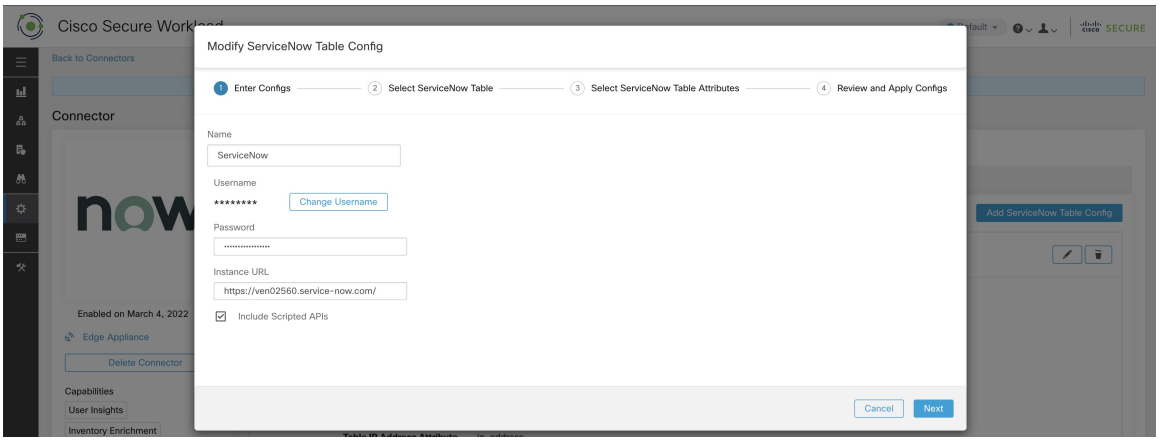


Figure 21: Cisco Secure Workload récupère les informations relatives aux tableaux de l'instance ServiceNow

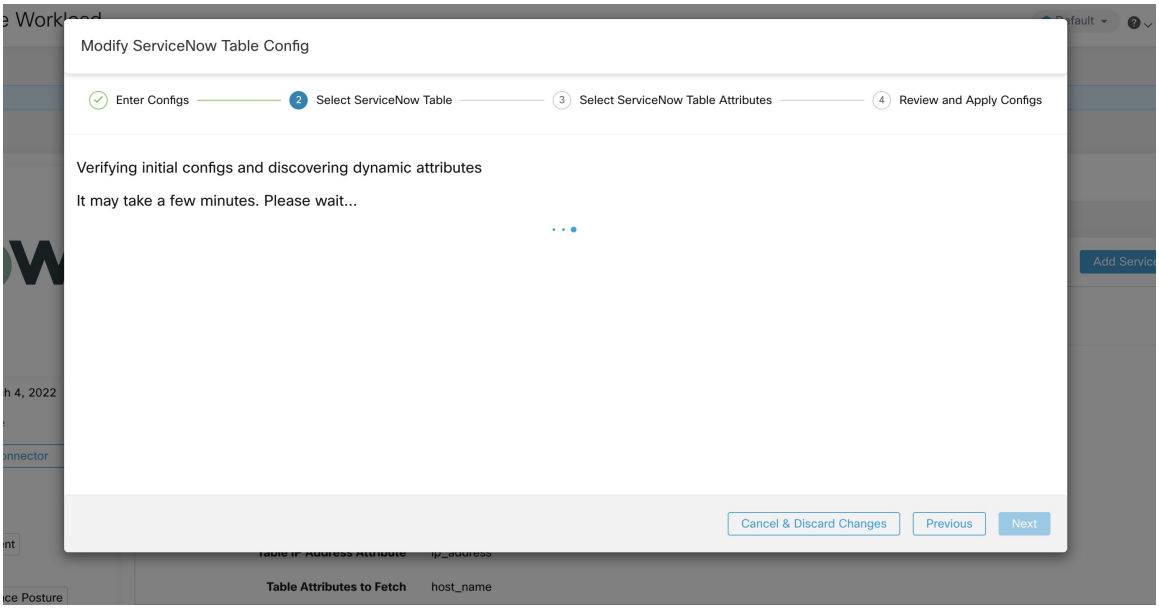


Figure 22: Cisco Secure Workload présente la liste des tableaux

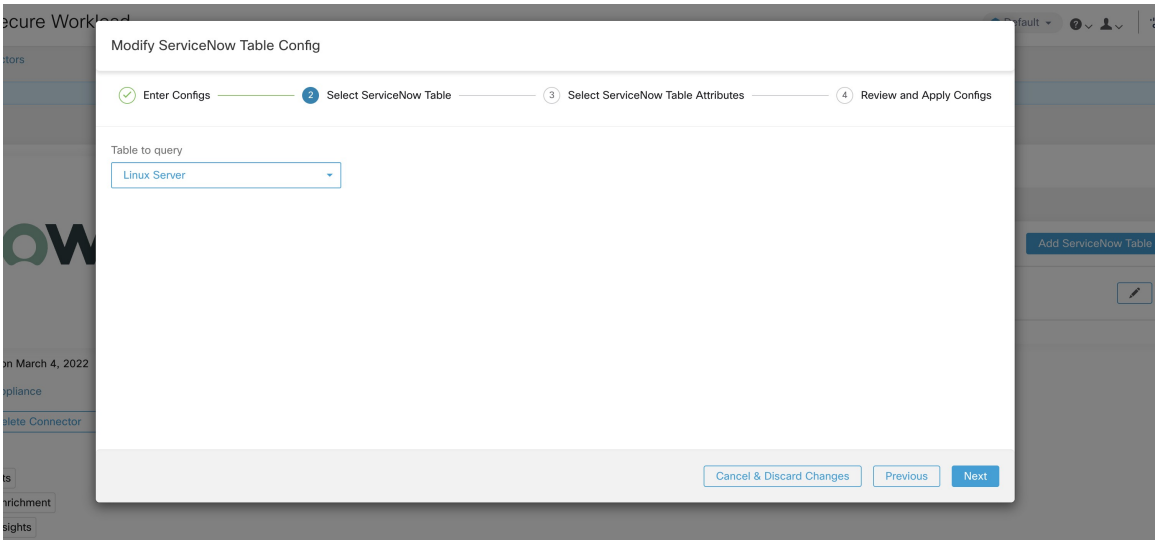


Figure 23: L'utilisateur sélectionne l'attribut ip_address et un autre attribut dans le tableau.

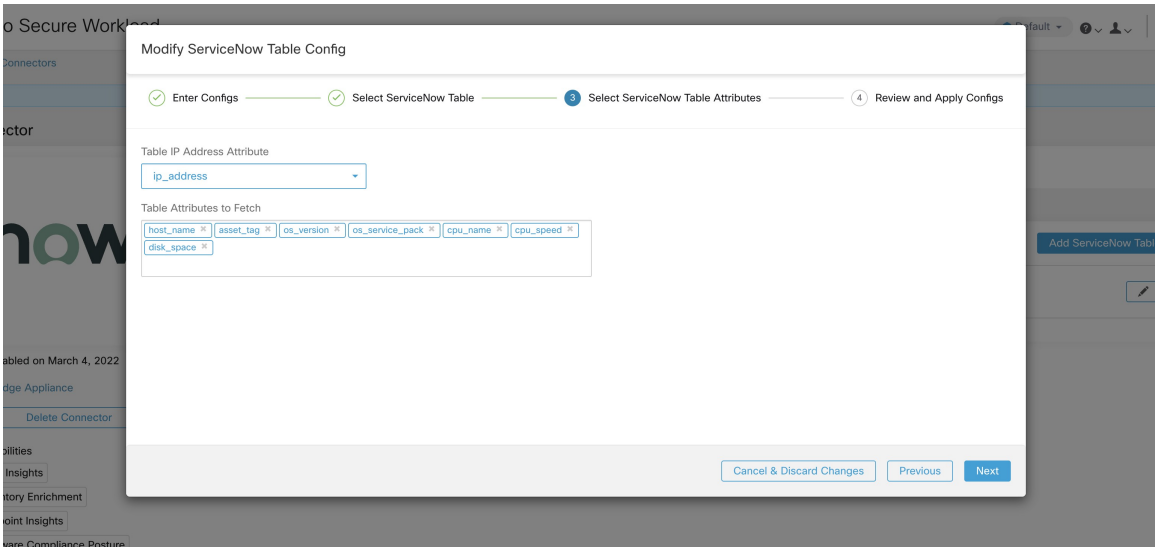
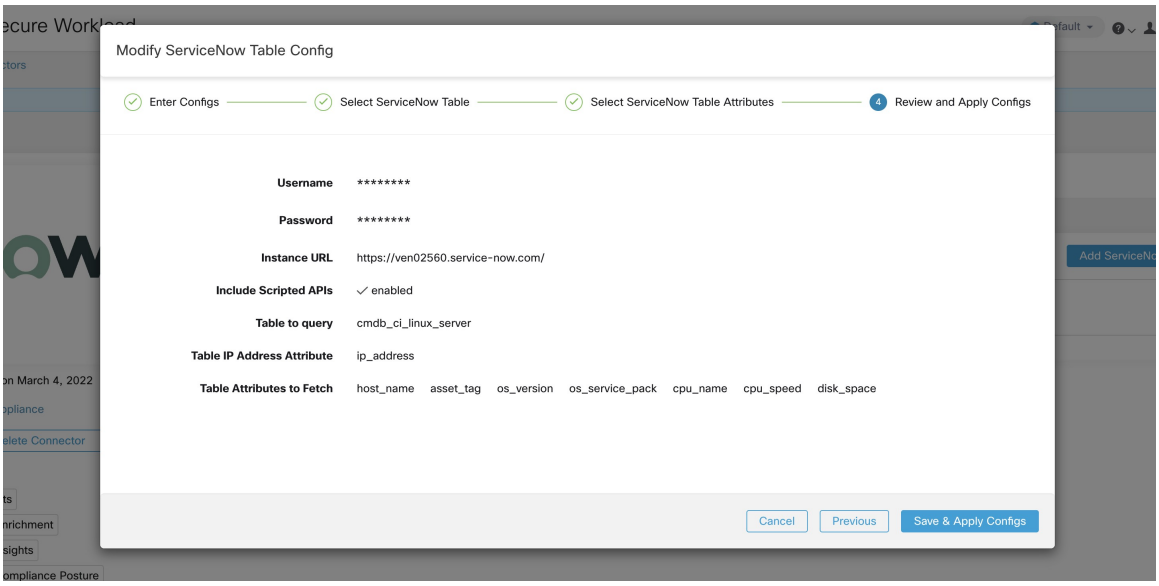


Figure 24: L'utilisateur finalise la configuration de ServiceNow.



Traitement des enregistrements ServiceNow

En fonction de l'URL d'instance que vous avez fournie lors de la configuration, le connecteur ServiceNow se connecte à l'instance ServiceNow. L'instance ServiceNow utilise des appels HTTP utilisant `https://{URL de l'instance}/api/new/doc/table/schema` pour obtenir le schéma de table initial à partir de l'API de la table ServiceNow. En fonction des tables configurées, il interroge ces tables pour récupérer les étiquettes et les métadonnées de ServiceNow. Cisco Secure Workload annote les étiquettes ServiceNow des adresses IP de son inventaire. Le connecteur ServiceNow récupère régulièrement de nouvelles étiquettes et met à jour l'inventaire Cisco Secure Workload .

Note Cisco Secure Workload récupère régulièrement les enregistrements des tables ServiceNow. Cela est configurable sous l'onglet SyncInterval dans le connecteur ServiceNow. L'intervalle de synchronisation par défaut est de 60 minutes. Pour les cas d'intégration de la table ServiceNow avec un grand nombre d'entrées, cet intervalle de synchronisation doit être défini à une valeur plus élevée.

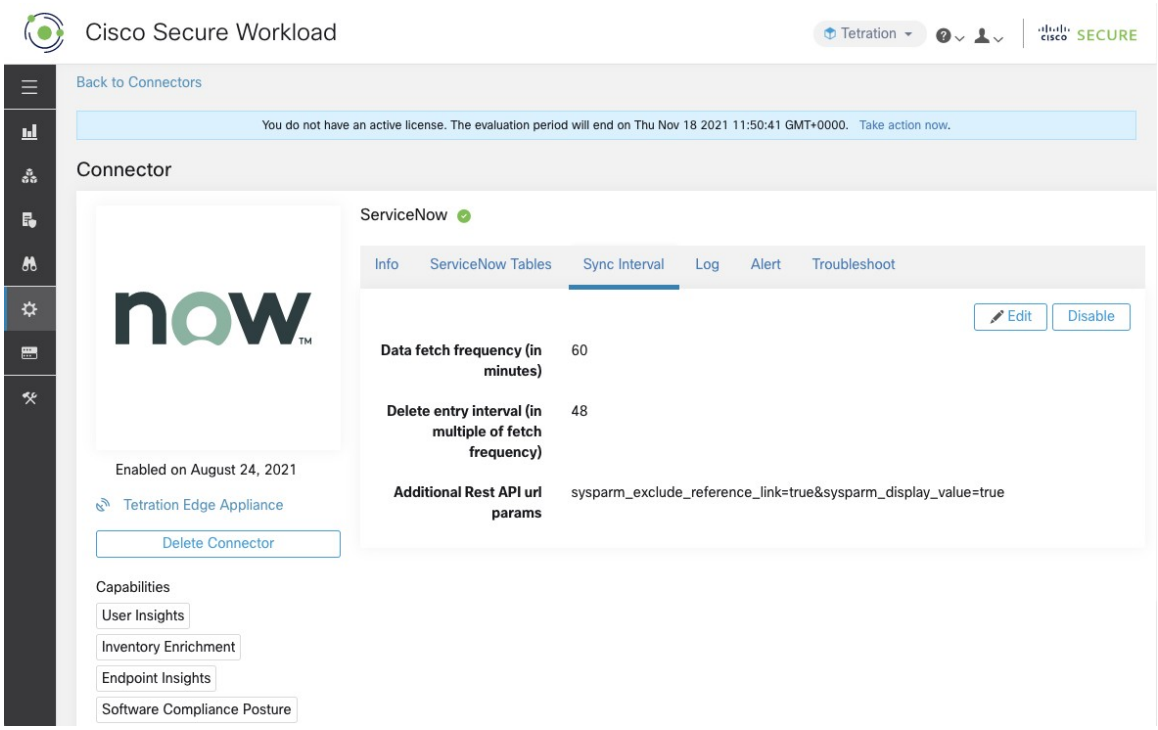
Note Cisco Secure Workload supprimera toute entrée non visible pendant 10 intervalles de synchronisation continus. Si la connexion à l'instance ServiceNow est interrompue pendant une période aussi longue, cela peut entraîner le nettoyage de toutes les étiquettes de cette instance.

Configuration de l'intervalle de synchronisation

1. Le connecteur ServiceNow de Cisco Secure Workload permet de configurer la fréquence de synchronisation entre Cisco Secure Workload et l'instance ServiceNow. Par défaut, l'intervalle de synchronisation est fixé à 60 minutes, mais il peut être modifié dans la configuration de l'intervalle de synchronisation sous la forme **Fréquence d'extraction des données**.

2. Pour détecter la suppression d'un enregistrement, le connecteur Cisco Secure Workload ServiceNow s'appuie sur les synchronisations des instances ServiceNow. Si une entrée n'est pas vue dans 48 intervalles de synchronisation consécutifs, nous supprimons l'entrée. Cela peut être configuré dans la configuration de l'intervalle de synchronisation sous la forme **Delete entry interval** (Supprimer l'intervalle d'entrée).
3. Si des paramètres supplémentaires doivent être transmis lors de l'appel des API REST pour les tableaux ServiceNow, vous pouvez les configurer dans le cadre des paramètres d'*URL supplémentaires de l'API REST*. Cette configuration est facultative. Par exemple, pour obtenir une recherche de référence à partir de ServiceNow, les paramètres d'URL suivants peuvent être utilisés **sysparm_exclude_reference_link=true&sysparm_display_value=vrai**

Figure 25: Configuration de l'intervalle de synchronisation



Commande Explore pour supprimer les étiquettes

Si l'utilisateur souhaite nettoyer les étiquettes pour une adresse IP particulière pour une instance donnée immédiatement, sans attendre l'intervalle de suppression, il peut le faire à l'aide de la commande explore. Voici les étapes à suivre pour exécuter la commande.

1. Recherche de l'ID VRF d'un détenteur
2. Accès à l'interface utilisateur de la commande Explore (Explorer)
3. Exécution des commandes

Recherche de l'ID VRF d'un détenteur

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Tenant** (Détenteur) sous le menu **platform** (plateforme) dans la barre de navigation à gauche de la

fenêtre. Cette page affiche tous les détenteurs et VRF actuellement configurés. Pour en savoir plus, consultez la section Détenteurs pour plus de détails.

Dans la page Détenteurs, le champ `ID` du tableau des détenteurs correspond à l'ID VRF du détenteur.

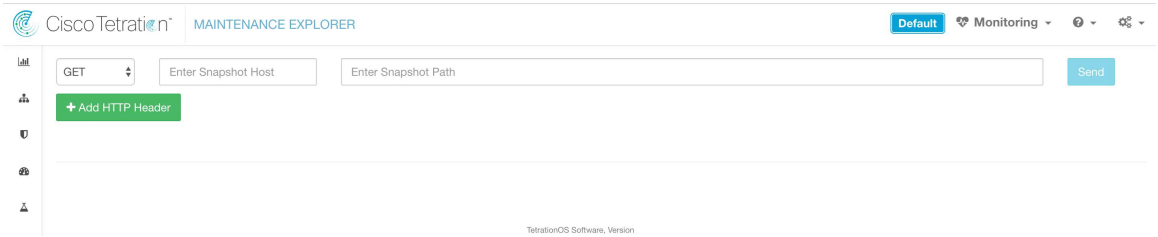
Accès à l'interface utilisateur de la commande Explore (Explorer)

Pour accéder à l'interface de commande Maintenance Explorer (Explorateur de maintenance), choisissez **Troubleshoot (Dépannage)** > **Maintenance Explorer (Explorateur de maintenance)** dans la barre de navigation de gauche de l'interface Web Cisco Secure Workload.

Note Des privilèges de service d'assistance à la clientèle sont nécessaires pour accéder au menu d'exploration. Si l'onglet d'exploration ne s'affiche pas, le compte n'a peut-être pas les autorisations nécessaires.

Cliquez sur l'onglet Explore (Explorer) dans le menu déroulant pour accéder à la page Maintenance Explorer (Explorateur de maintenance).

Figure 26: Onglet Maintenance Explorer (Explorateur de maintenance)



Exécution des commandes

- Choisissez l'action `POST`
- Saisissez l'hôte de l'instantané en tant que `orchestrator.service.consul`
- Saisir le chemin d'accès à l'instantané

  Pour supprimer les étiquettes d'une adresse IP particulière pour une `instance ServiceNow, procédez comme suit : servicenow_cleanup_annotations?args=<vrf-id> <ip_address> <instance_url> <table_name>`
- Cliquez sur Envoyer

Remarque Si, après avoir été supprimé à l'aide de la commande explore, l'enregistrement apparaît dans l'instance de ServiceNow, il sera réalimenté.

Foire aux questions

1. **Que faire si la table de CMDB ServiceNow ne comporte pas d'adresse IP.**

Dans ce cas, il est recommandé de créer une vue sur ServiceNow qui contiendra les champs souhaités de la table actuelle ainsi que l'adresse IP (provenant potentiellement d'une opération JOIN avec une autre table). Une fois qu'une telle vue est créée, elle peut être utilisée à la place du nom de table.

2. **Que se passe-t-il si l'instance ServiceNow nécessite une authentification multifactorielle**

   Actuellement, nous ne prenons pas en charge l'intégration de l'instance ServiceNow avec l'authentification multifactorielle.

Limites

Unité	Limite
Nombre maximal d'instances ServiceNow qui peuvent être configurées sur un connecteur ServiceNow	20
Nombre maximal d'attributs qui peuvent être extraits d'une instance de ServiceNow	10
Nombre maximal de connecteurs ServiceNow sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs ServiceNow sur un détenteur (portée racine)	1
Nombre maximal de connecteurs ServiceNow sur Cisco Secure Workload	150

Connecteurs pour les notifications d'alertes

Les connecteurs pour les notifications d'alertes permettent à Cisco Secure Workload de publier des alertes Cisco Secure Workload sur diverses plateformes de messagerie et de journalisation. Ces connecteurs fonctionnent sur le service TAN sur l'appareil de périphérie Cisco Secure Workload.

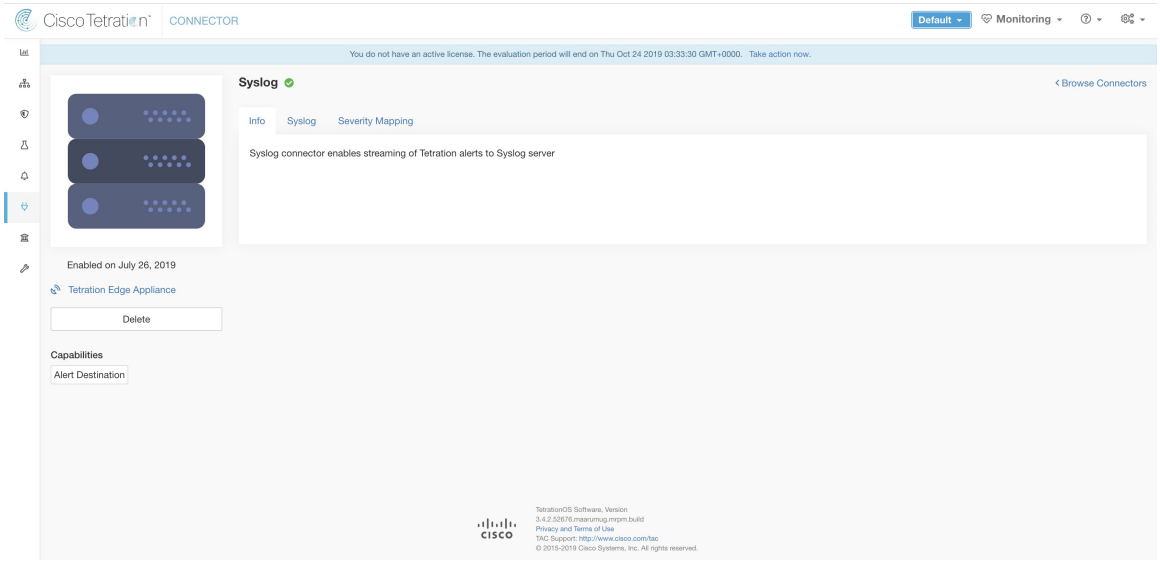
Connecteur	Description	Déployé sur une appliance virtuelle
Syslog	Envoyer des alertes Cisco Secure Workload au serveur Syslog.	Cisco Secure Workload Edge
Email	Envoyer des alertes Cisco Secure Workload par courriel	Cisco Secure Workload Edge
Slack	Envoyez des alertes Cisco Secure Workload sur Slack.	Cisco Secure Workload Edge
PagerDuty	Envoi d'alertes Cisco Secure Workload sur Pager Duty.	Cisco Secure Workload Edge
Kinesis	Envoyez des alertes Cisco Secure Workload sur Amazon Kinesis.	Cisco Secure Workload Edge

Pour en savoir plus sur les appliances virtuelles nécessaires, consultez la section Appliances virtuelles pour les connecteurs.

Connecteur Syslog

Lorsqu'activé, le service TAN (Outil de notification d'alertes) sur l'appareil de périphérie Cisco Secure Workload de Cisco peut envoyer des alertes au serveur Syslog à l'aide de la configuration.

Figure 27: Connecteur syslog



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur le serveur Syslog. Pour plus d'informations, consultez la Configuration de l'outil de notification Syslog.

Nom du paramètre	Type	Description
Protocol	Liste déroulante	Protocole à utiliser pour la connexion au serveur
	•*UDP*	
	• *TCP*	
Adresse du serveur	chaîne	Nom d'hôte ou adresse IP du serveur Syslog.
Port	number	Port d'écoute du serveur Syslog. La valeur du port par défaut est 514.

Figure 28: Exemple de configuration pour le connecteur Syslog

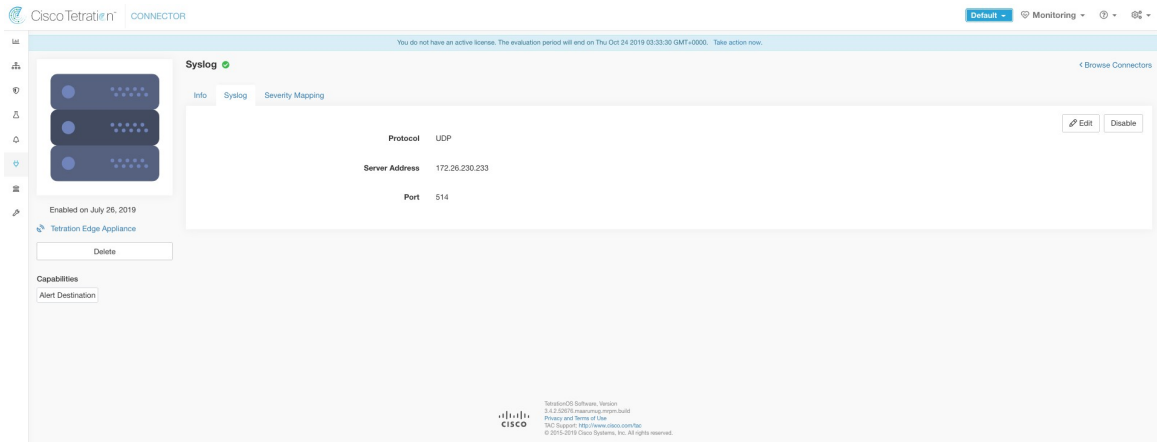


Figure 29: Exemple d'alerte

Mappage de gravité Syslog

Le tableau suivant présente le mappage de gravité par défaut pour les alertes Cisco Secure Workload dans Syslog.

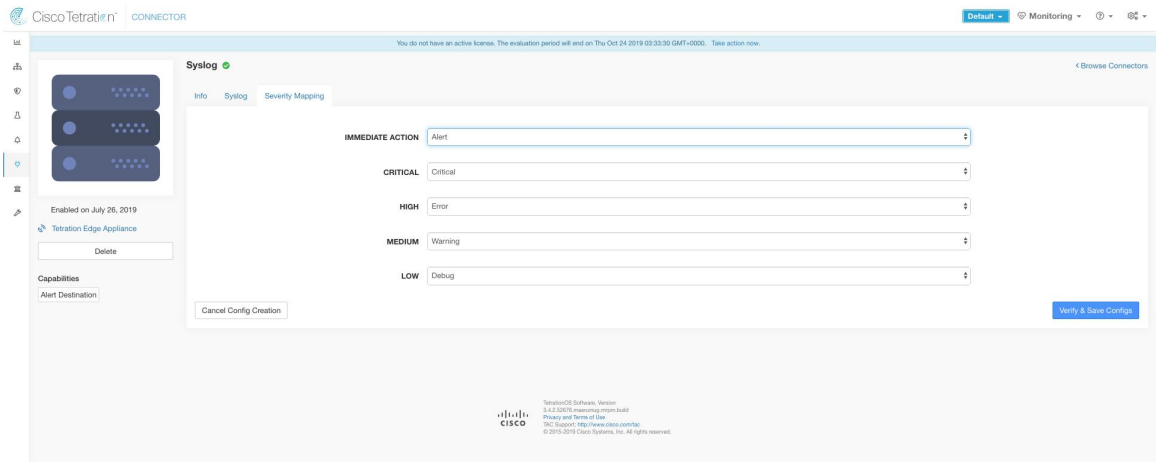
Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
FAIBLE	LOG_DEBUG
MOYENNE	LOG_WARNING
ÉLEVÉE	LOG_ERR
CRITIQUE	JOURNAL_CRIT

Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
ACTION IMMÉDIATE	LOG_EMERG

Ce paramètre peut être modifié à l'aide de la configuration du **Mappage de la gravité** du connecteur Syslog. Vous pouvez choisir la priorité Syslog correspondante pour chaque gravité d'alerte Cisco Secure Workload et modifier le mappage des gravités. Pour plus d'informations, consultez Configuration du mappage de gravité Syslog.

Nom du paramètre	Liste déroulante des mappages
ACTION_IMMÉDIATE	• *Urgence* • *Alerte* • *Critique* • *Erreur* • *Avertissement* • *Avis* • *Information* • *Débogage*
CRITIQUE	
ÉLEVÉ	
MOYENNE	
FAIBLE	

Figure 30: Exemple de configuration pour le mappage de gravité Syslog



Limites

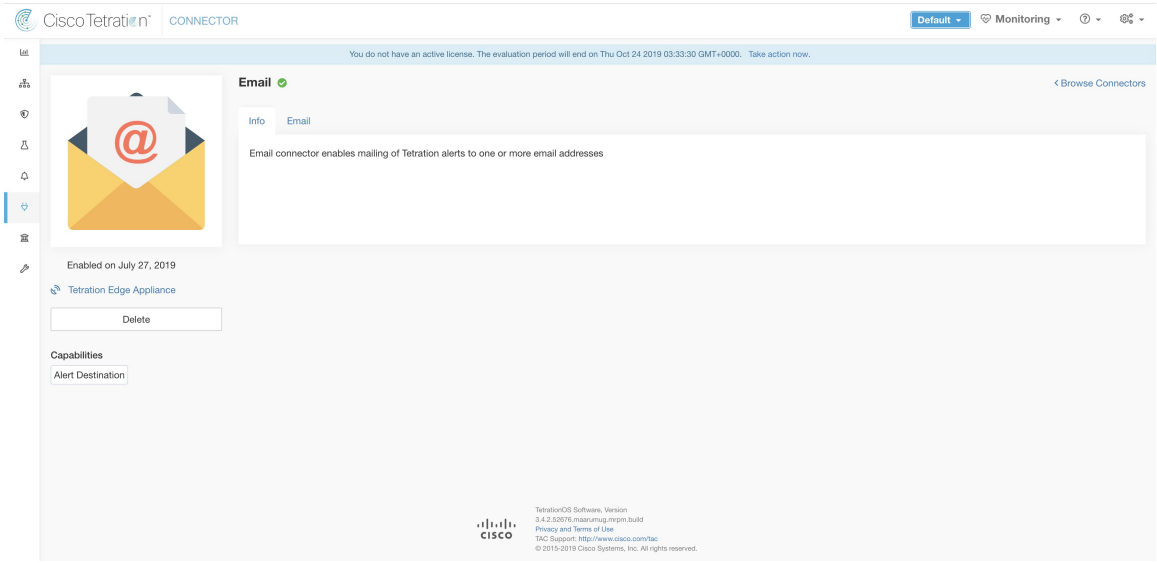
Unité	Limite
Nombre maximal de connecteurs Syslog sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Syslog sur un détenteur (portée racine)	1

Unité	Limite
Nombre maximal de connecteurs Syslog sur Cisco Secure Workload	150

Connecteur de courriel

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes pour une configuration donnée.

Figure 31: Connecteur de courriel



Le tableau suivant explique les détails de configuration pour la publication d'alertes Cisco Secure Workload dans des courriels. Pour en savoir plus, consultez la Configuration de l'outil de notification des courriels.

Table 3: Configuration du notificateur par courriel pour plus de détails

Nom du paramètre	Type	Description
Nom d'utilisateur SMTP	chaîne	Nom d'utilisateur du serveur SMTP Ce paramètre est facultatif.
Mot de passe SMTP	chaîne	Mot de passe du serveur SMTP pour l'utilisateur (si fourni) Ce paramètre est facultatif.
SMTP Server	chaîne	Nom d'hôte ou adresse IP du serveur SMTP
Port SMTP	number	Port d'écoute du serveur SMTP. La valeur par défaut est 587.
Connection sécurisée	case	Doit-on utiliser SSL pour la connexion au serveur SMTP?

Nom du paramètre	Type	Description
Adresse courriel d'expédition	chaîne	Adresse courriel à utiliser pour l'envoi des alertes
Destinataires par défaut	chaîne	Liste d'adresses courriel de destinataires séparées par des virgules

Figure 32: Exemple de configuration pour un connecteur par courriel

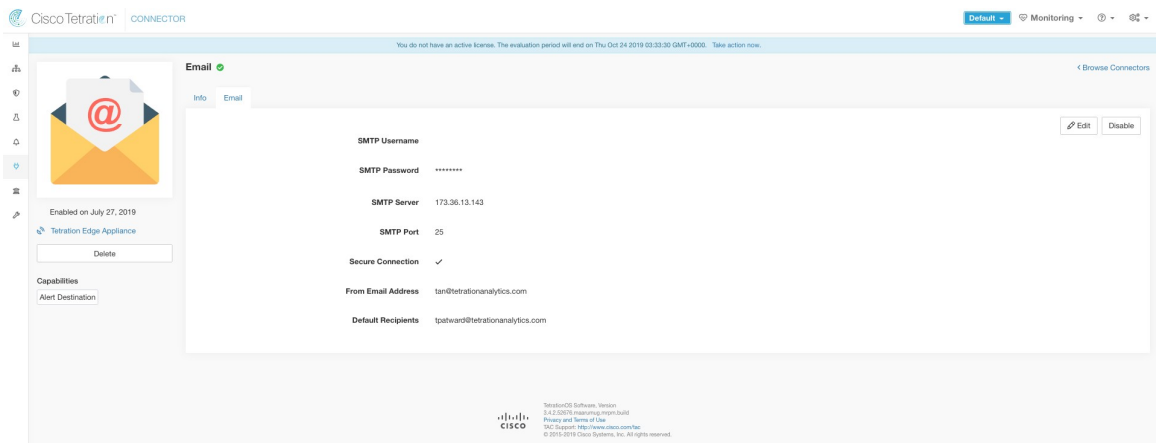
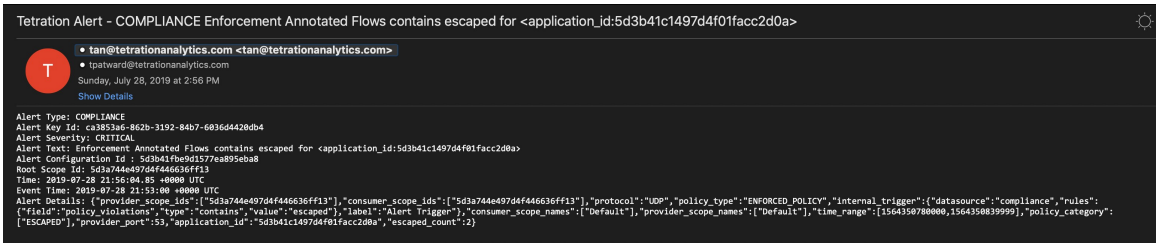


Figure 33: Exemple d'alerte



Note

- Le nom d'utilisateur et le mot de passe SMTP sont facultatifs. Si aucun nom d'utilisateur n'est fourni, nous essayons la connexion au serveur SMTP sans aucune authentification.
- Si la case de la connexion sécurisée n'est pas cochée, nous enverrons une notification d'alerte de connexion non sécurisée.
- La liste des destinataires par défaut est utilisée pour envoyer des notifications d'alertes. Cela peut être remplacé par alerte si la configuration des alertes l'exige.

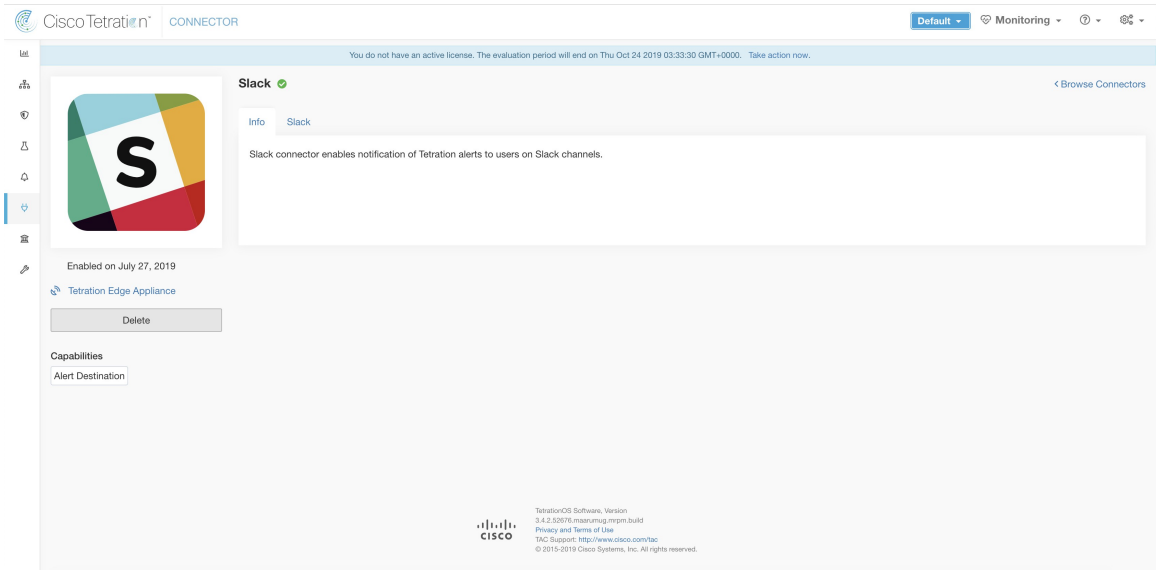
Limites

Unité	Limite
Nombre maximal de connecteurs de courriel sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs de courriel sur un détenteur (portée racine)	1
Nombre maximal de connecteurs de courriel sur Cisco Secure Workload	150

Connecteur Slack

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à Slack à l'aide de la configuration.

Figure 34: Connecteur Slack



Le tableau suivant explique les détails de la configuration pour la publication des alertes Cisco Secure Workload sur Slack. Pour en savoir plus, consultez la Configuration de l'outil de notification Slack.

Nom du paramètre	Type	Description
URL de point d'ancrage Web Slack	chaîne	Point d'ancrage Web Slack sur lequel les alertes Cisco Secure Workload doivent être publiées

Note

- Pour générer un point d'ancrage Web Slack, cliquez ici.

Figure 35: Exemple de configuration pour le connecteur Slack

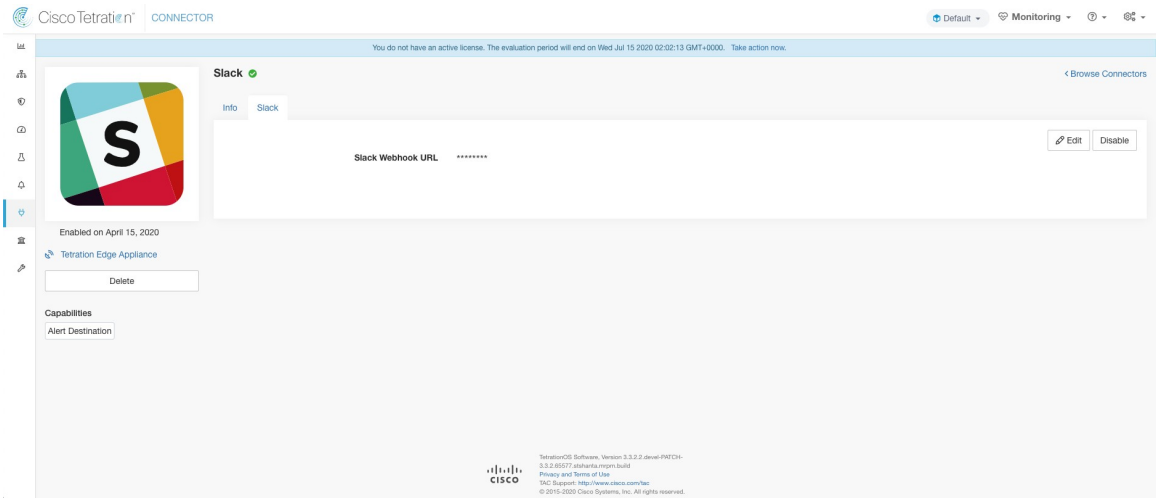
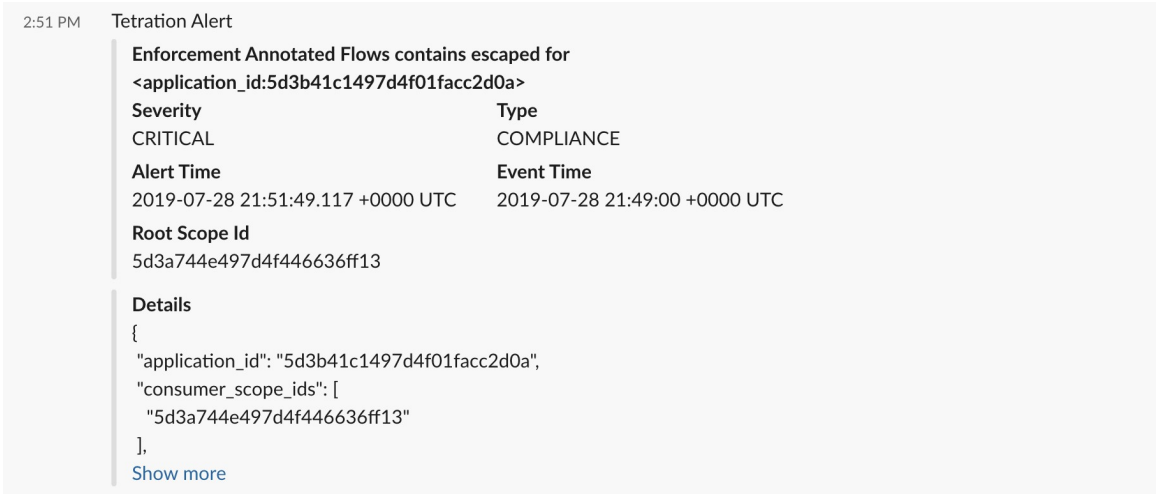


Figure 36: Exemple d'alerte



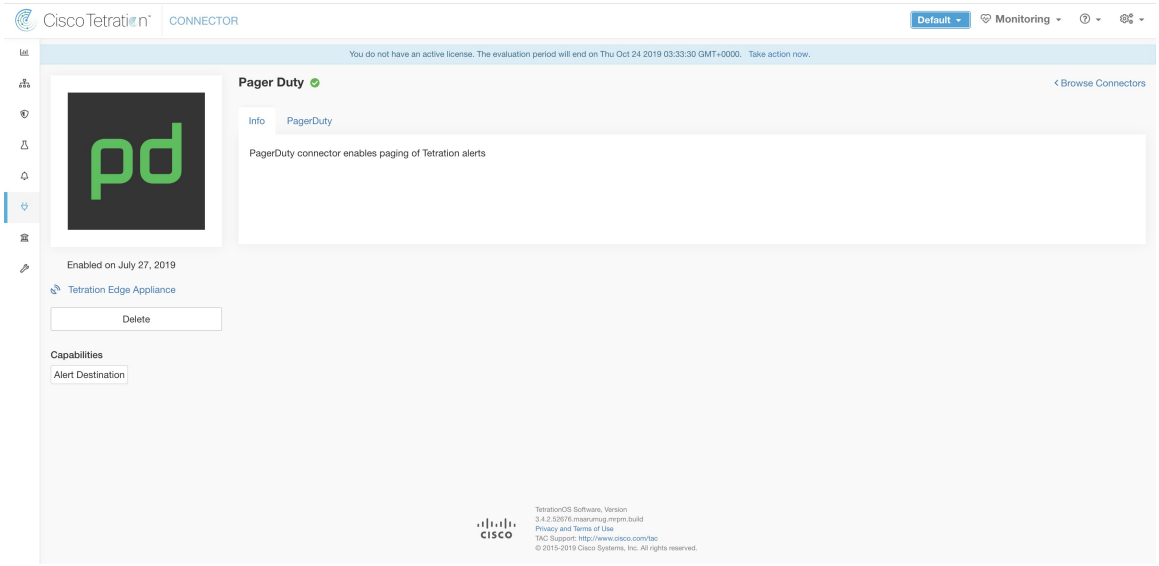
Limites

Unité	Limite
Nombre maximal de connecteurs Slack sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Slack sur un détenteur (portée racine)	1
Nombre maximal de connecteurs Slack sur Cisco Secure Workload	150

Connecteur PagerDuty

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à PagerDuty à l'aide de la configuration.

Figure 37: Connecteur PagerDuty



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur PagerDuty. Pour en savoir plus, consultez Configuration de l'outil de notification PagerDuty.

Nom du paramètre	Type	Description
Clé de service PagerDuty	chaîne	Clé de service PagerDuty pour activer les alertes Cisco Secure Workload sur PagerDuty.

Figure 38: Exemple de configuration pour PagerDuty Connector

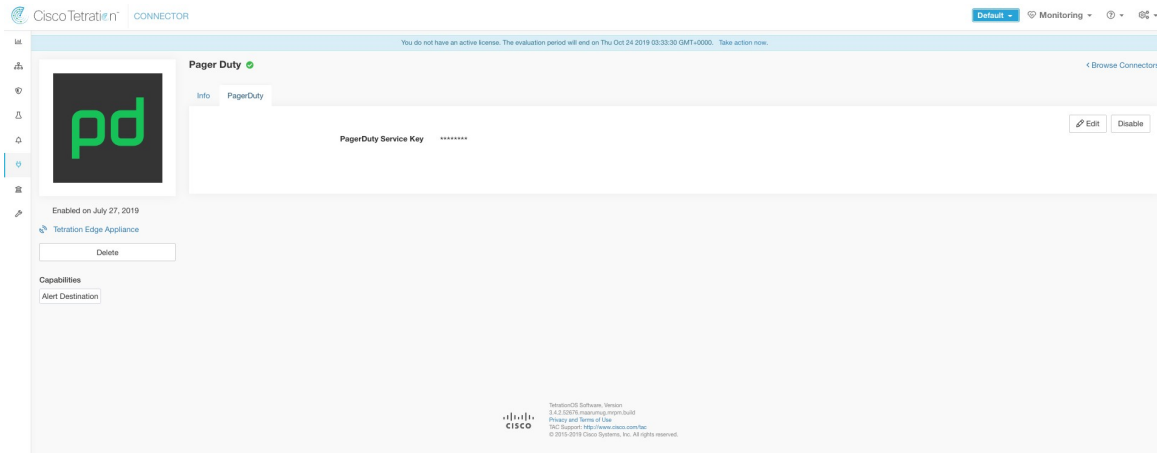
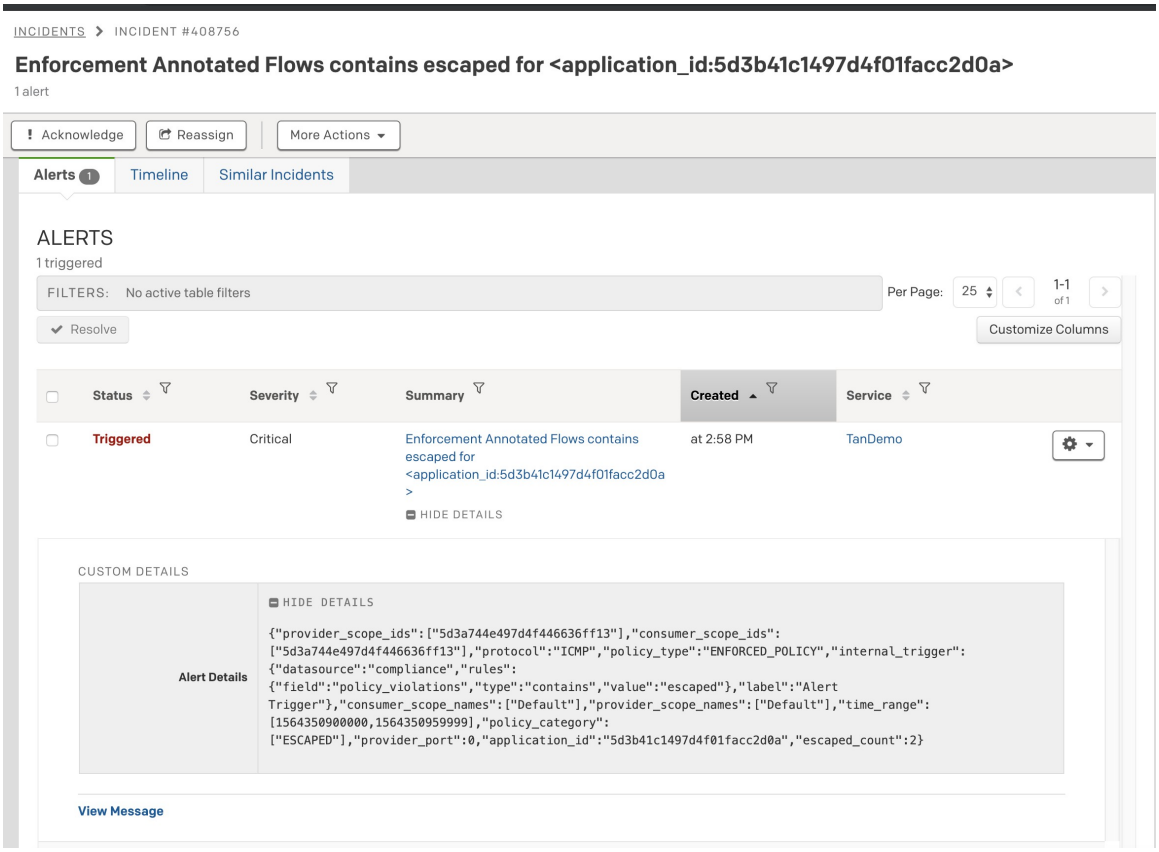


Figure 39: Exemple d'alerte



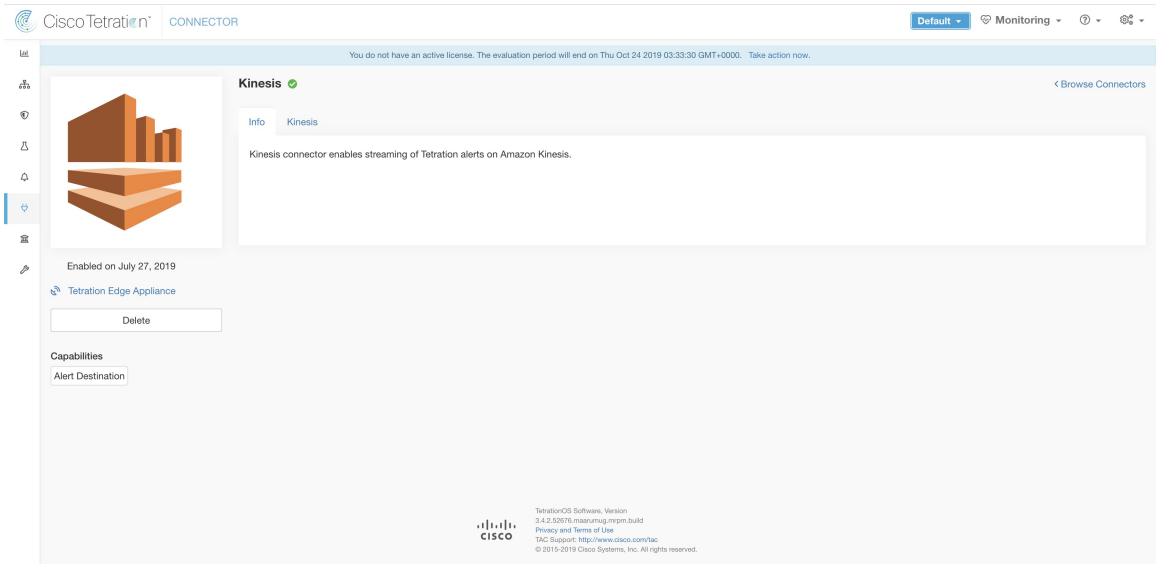
Limites

Unité	Limite
Nombre maximal de connecteurs PagerDuty sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs PagerDuty sur un détenteur (portée racine)	1
Nombre maximal de connecteurs PagerDuty sur Cisco Secure Workload	150

Connecteur Kinesis

Lorsqu'activé, le service TAN sur l'appareil de périphérie Cisco Secure Workload peut envoyer des alertes à l'aide de la configuration.

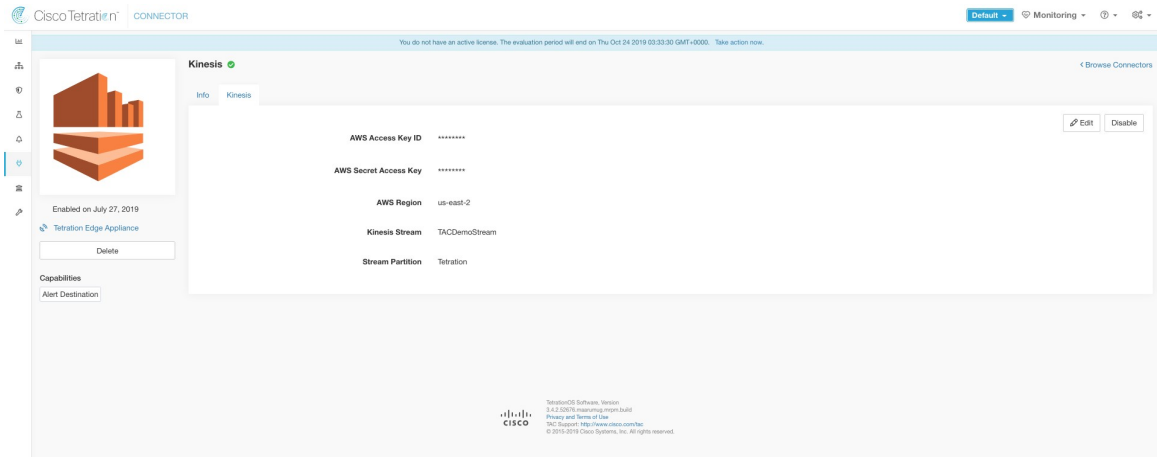
Figure 40: Connecteur Kinesis



Le tableau suivant explique les détails de configuration pour la publication des alertes Cisco Secure Workload sur Amazon Kinesis. Pour en savoir plus, consultez la Configuration de l'outil de notification Kinesis.

Nom du paramètre	Type	Description
ID de la clé d'accès AWS	chaîne	ID de clé d'accès AWS pour communiquer avec AWS
Clé d'accès secrète AWS	chaîne	Clé d'accès secrète AWS pour communiquer avec AWS
Région AWS	dropdown of AWS regions	Nom de la région AWS où le flux Kinesis est configuré
Kinesis Stream	chaîne	Nom du flux Kinesis
Stream Partition	chaîne	Nom de la partition du flux

Figure 41: Exemple de configuration pour le connecteur Kinesis



Limites

Unité	Limite
Nombre maximal de connecteurs Kinesis sur un appareil de périphérie Cisco Secure Workload	1
Nombre maximal de connecteurs Kinesis sur un détenteur (portée racine)	1
Nombre maximal de connecteurs Kinesis sur Cisco Secure Workload	150

connecteurs infonuagiques

Vous pouvez utiliser un connecteur infonuagique pour les fonctionnalités Cisco Secure Workload sur les charges de travail infonuagique.

Les connecteurs infonuagiques ne nécessitent pas d'appliance virtuelle.

Connecteur	Fonctionnalités prises en charge	Déployé sur une appliance virtuelle
AWS	Pour les VPC Amazon Web Services : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes EKS (Elastic Kubernetes Service) : • Recueillir des métadonnées	S. O.
Azure	Pour les réseaux virtuels Azure : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes Azure Kubernetes Service (AKS) : • Recueillir des métadonnées	S. O.
GCP	Pour les VPC Google Cloud Platform : • Recueillir les métadonnées (étiquettes) • Recueillir les journaux de flux • Appliquer les politiques de segmentation À partir des grappes de Google Kubernetes Engine (GKE) : • Recueillir les métadonnées (étiquettes)	s.o.

Connecteur AWS

Le connecteur Amazon Web Services (AWS) se connecte à AWS pour remplir les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses étiquettes) en direct à partir d'un nuage privé virtuel (VPC)** AWS; AWS vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload interroger les balises de ces ressources qui peuvent ensuite être utilisées pour la visualisation des données d'inventaire et des flux de trafic, et pour la définition de politiques. Cette fonctionnalité maintient le mappage des balises de ressources à jour en synchronisant constamment ces données.

  Les balises des charges de travail et des interfaces réseau d'un AWS VPC sont acquises. Si vous configurez à la fois des charges de travail et des interfaces réseau, Cisco Secure Workload fusionne et affiche les balises. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques.

- **Acquisition de journaux de flux VPC** Si vous avez configuré les journaux de flux VPC dans AWS à des fins de surveillance, Cisco Secure Workload peut acquérir des informations des journaux de flux en lisant le compartiment S3 correspondant. Vous pouvez utiliser cette télémétrie pour la génération de politiques de visualisation et de segmentation.

- **Segmentation** Lorsque l'option de segmentation est activée, Cisco Secure Workload programme les politiques de sécurité à l'aide des groupes de sécurité natifs d'AWS. Lorsque la mise en application est activée pour un VPC, les politiques pertinentes sont automatiquement programmées en tant que groupes de sécurité.

- **Acquisition automatisée des métadonnées des grappes EKS** Lorsque Elastic Kubernetes Services (EKS) est exécuté sur AWS, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et de pods associées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir les fonctionnalités à activer pour chaque VPC.

Note Nous ne prenons pas actuellement en charge les régions de la Chine.

Exigences et prérequis AWS

Pour toutes les fonctionnalités : créez un utilisateur dédié dans AWS ou identifiez un utilisateur AWS existant pour ce connecteur. L'assistant de configuration du connecteur génère un modèle de formation de nuage CloudFormation (CFT) que vous pouvez utiliser pour attribuer les privilèges requis à cet utilisateur. Assurez-vous que vous avez les autorisations dans AWS pour charger ce CFT.

Pour accorder un accès multicompte AWS à l'utilisateur dédié, consultez (Facultatif) Configurer l'accès multicompte AWS dans AWS, on page 69, y compris les privilèges d'accès requis.

Pour accorder l'accès au compte AWS à l'aide du rôle, consultez la section accès basé sur les rôles à la grappe Cisco Secure Workload.

Chaque VPC ne peut appartenir qu'à un seul connecteur AWS. Une grappe Cisco Secure Workload peut avoir plusieurs connecteurs AWS. Rassemblez les informations décrites dans les tableaux de la Configurer un nouveau connecteur AWS , on page 73.

Ce connecteur ne nécessite pas d'appliance virtuelle.

Pour la collecte d'étiquettes et de l'inventaire : aucune condition préalable supplémentaire n'est requise.

Pour l'acquisition des journaux de flux : des définitions de journaux de flux au niveau VPC sont requises pour déclencher la collecte des journaux de flux.

Seuls les journaux de flux de niveau VPC peuvent être intégrés.

Les journaux de flux doivent être publiés dans Amazon Simple Storage Service (S3). Cisco Secure Workload ne peut pas collecter de données de flux à partir des journaux Amazon CloudWatch.

Secure Workload peut acquérir des journaux de flux d'un compartiment S3 associé à n'importe quel compte, si les informations d'authentification du compte d'utilisateur AWS fournies lors de la création du connecteur ont accès à la fois aux journaux de flux VPC et au compartiment S3.

Les attributs de journal de flux suivants (dans n'importe quel ordre) sont requis dans ce dernier : adresse source, adresse de destination, port source, port de destination, protocole, paquets, octets, heure de début, heure de fin, action, indicateurs TCP, ID d'interface, État du journal et direction du flux. Tout autre attribut est ignoré.

Les journaux de flux doivent saisir le trafic autorisé et refusé.

Note Le connecteur Cisco Secure Workload AWS prend en charge la partition des journaux de flux VPC sur une base horaire et quotidienne.

Pour la segmentation : l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Sauvegardez vos groupes de sécurité existants avant d'activer la segmentation du connecteur, car toutes les règles existantes sont remplacées lorsque vous activez la segmentation pour un VPC.

Pour en savoir plus, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.

Pour les services Kubernetes gérés (EKS) : si vous activez l'option Kubernetes, consultez Exigences et prérequis EKS dans la section des services Kubernetes gérés fonctionnant sur AWS (EKS), y compris les privilèges d'accès requis.

(Facultatif) Configurer l'accès multicompte AWS dans AWS

Si les renseignements d'authentification utilisateur fournis ont accès aux VPC appartenant à d'autres comptes AWS, ces derniers seront disponibles pour traitement dans le cadre du connecteur AWS.

1. L'utilisateur Cisco Secure Workload désigné doit disposer des autorisations d'accès AWS suivantes :

```
1. iam:GetPolicyVersion
2. iam:ListPolicyVersions
3. iam:ListAttachedUserPolicies
4. iam:GetUser
5. servicequotas:ListServiceQuotas
```

Exemple JSON de politique AWS :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:ListPolicyVersions",
        "iam:ListAttachedUserPolicies",
        "iam:GetUser",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

2. Créez un rôle IAM AWS dans le compte AWS souhaité dont l'utilisateur Cisco Secure Workload désigné ne fait PAS partie.
3. Autorisez que le rôle AWS IAM soit assumé par l'utilisateur Cisco Secure Workload. Cela peut être fait en ajoutant l'ARN de l'utilisateur Cisco Secure Workload à la politique d'approbation du rôle IAM d'AWS.

   Exemple JSON de politique d'approbation de rôle IAM AWS :

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": <Secure Workload_user_arn>
            },
  "Action": "sts:AssumeRole",
  "Condition": {}
    }
  ]
}
```

4. Exécutez les étapes 2 et 3 pour tous les comptes AWS souhaités auxquels l'utilisateur Cisco Secure Workload n'appartient pas.
5. Créez une politique gérée par le client (PAS une politique en ligne) avec l'autorisation d'assumer tous les rôles AWS créés à partir de différents comptes.

Remarque Dans le connecteur AWS, la politique en ligne du client n'est pas prise en charge.

Exemple de politique gérée JSON :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [<AWS_role_cross_account_1_arn>, <AWS_role_cross_account_2_arn>...]
    }
  ]
}
```

6. Associez la politique gérée par le client créée à l'utilisateur Cisco Secure Workload.
7. L'assistant de configuration du connecteur fournit un modèle CloudFormation. Après avoir téléchargé la CFT telle quelle sur l'utilisateur Cisco Secure Workload désigné, vous modifierez le modèle et vous téléchargerez le modèle modifié sur le portail CloudFormation pour accorder les autorisations requises pour les rôles AWS IAM. Pour en savoir plus, consultez Configurer un nouveau connecteur AWS , à la page 73.

Authentification à l'aide de rôles

L'authentification basée sur l'utilisateur nécessite des clés d'authentification. Une clé d'authentification mal gérée peut constituer une menace pour la sécurité en raison de sa nature sensible.

L'utilisation de l'authentification basée sur les rôles vous permet de configurer le compte AWS à l'aide de rôles. La configuration du connecteur accepte l'identifiant du rôle (ARN) et assume ce rôle pour effectuer des actions spécifiques sur le compte du client.

L'authentification basée sur les rôles réduit le risque d'accès non autorisé.

Pour accéder à l'authentification basée sur les rôles, procédez comme suit :

Procédure

Étape 1 Cliquez sur l'onglet **Role** (Rôle) dans la page de configuration du connecteur.

Étape 2 Enregistrez la grappe. Si la grappe n'est pas enregistrée, elle affiche le message *« Cluster is not registered to use role credentials (La grappe n'est pas enregistrée pour utiliser les informations d'authentification du rôle) ». Téléchargez la charge utile fournie et communiquez avec un représentant du service d'assistance à la clientèle.*.

Étape 3 Dans le message de notification, cliquez sur le bouton de **Download** (Téléchargement) et téléchargez le fichier de charge utile.

Étape 4 Vous pouvez utiliser le lien dans le message de notification pour contacter l'équipe **TAC**, créer le dossier et fournir le fichier que vous avez téléchargé.

Étape 5 Lorsque la grappe est enregistrée, l' **ID externe** et **l'ARN de l'utilisateur** sont remplis automatiquement.

Remarque Actualisez la page pour afficher l'ID externe et l'ARN de l'utilisateur.

Étape 6 Utilisez l' **ID externe** et **l'ARN utilisateur** générés pour mettre à jour la relation d'approbation de rôle. Elle permet d'assumer le rôle.

La même partie du fichier JSON :

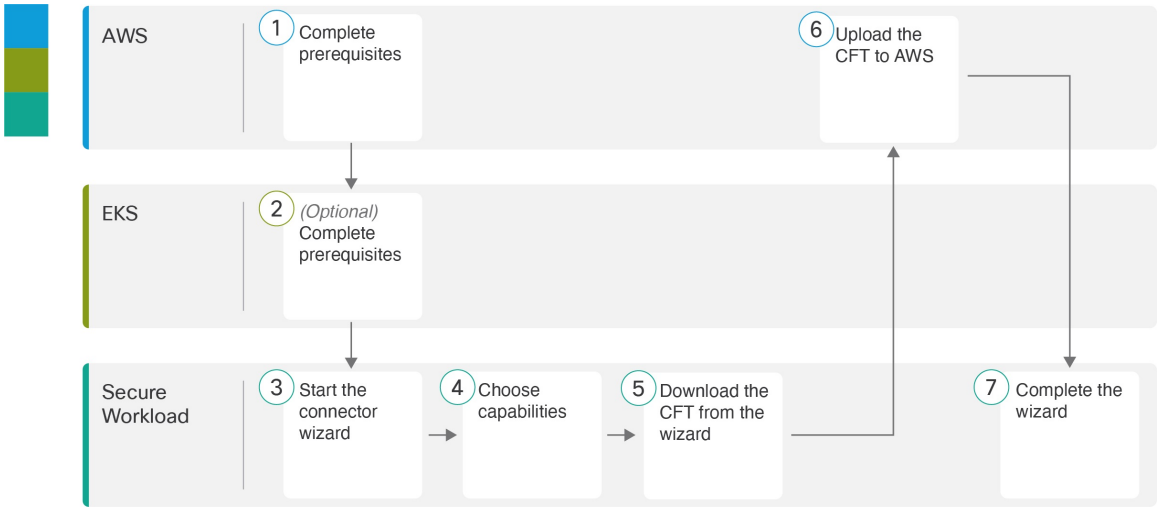
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "<User ARN>"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "<External Id>"
        }
      }
    }
  ]
}
```

Étape 7 Lorsque l'étape précédente est terminée, vous pouvez copier l' **ARN de rôle** du compte AWS et le coller dans la page de configuration du connecteur AWS.

Aperçu de la configuration du connecteur AWS

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour obtenir des renseignements essentiels, consultez la rubrique suivante (Configurer un nouveau connecteur AWS , à la page 73)

Illustration 42 : Aperçu de la configuration du connecteur AWS



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un nouveau connecteur AWS

Procédure

Étape 1 Dans le volet de navigation, choisissez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **AWS Connector** (Connecteur AWS).

Étape 3 Cliquez sur **Generate Template** (générer un modèle) et sélectionnez les fonctionnalités souhaitées.

En fonction des capacités sélectionnées, un modèle CloudFormation (FormationNuage) (CFT) est généré. Utilisez le modèle CFT généré dans votre CloudFormation AWS pour créer la politique pour l'utilisateur ou le rôle.

Pour activer la segmentation, vous devez également cocher**Gather Labels** (Regrouper les étiquettes).

Étape 4 Téléchargez le modèle CloudFormation (CFT) généré. Le CFT généré peut être utilisé à la fois pour l'utilisateur et le rôle.

Ce modèle dispose des privilèges IAM requis pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option Kubernetes, vous devez configurer séparément les autorisations pour EKS. Consultez Services gérés Kubernetes s'exécutant sur AWS (EKS), à la page 79.

Étape 5 Chargez le CFT sur le portail AWS CloudFormation pour attribuer des privilèges à l'utilisateur pour ce connecteur. Assurez-vous que l'utilisateur AWS dispose des privilèges requis avant de pouvoir continuer la configuration du connecteur AWS.

Remarque Nous vous recommandons d'effectuez cette opération, que vous utilisiez ou non l'accès entre comptes AWS.

Vous pouvez appliquer le CFT à l'aide du portail ou de la CLI. Pour en savoir plus, consultez ;

- **Portail :** AWS Management Console
- **CLI :** Création d'une pile

Lorsque vous chargez le CFT, AWS exige les détails suivants :

1. Nom de la politique (il peut s'agir de n'importe quel nom. Par exemple, connecteur Cisco Secure Workload)
2. Nom du rôle : nom du rôle IAM AWS auquel vous appliquez le CFT
3. Liste des ARN de compartiment et des ARN d'objet (par défaut : *)
4. Nom de l'utilisateur : nom de l'utilisateur AWS auquel vous appliquez le CFT
5. Liste des ARN de VPC (par défaut : *)

   Pour saisir une liste spécifique d'ARN de VPC, saisissez les ressources du groupe de sécurité et de l'interface réseau jumelées avec le VPC spécifique pour activer la segmentation.

   1. `arn:aws:ec2:<region>:<account_id>:security-group/*`
   2. `arn:aws:ec2:<region>:<account_id>:network-interface/*`

Exemple de code

Exemple 1

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:us-east-1:123456789:security-group/*",
    "arn:aws:ec2:us-east-1:123456789:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

Exemple 2

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

Étape 6 Si vous utilisez l'authentification basée sur les rôles d'AWS pour vous connecter au connecteur Cisco Secure Workload, consultez la section Rôles et privilèges d'accès EKS.

Étape 7 Si vous utilisez l'accès entre comptes AWS, suivez ces étapes supplémentaires :

1. Vous pouvez utiliser le même CFT téléversé pour donner accès au rôle ou à l'utilisateur. Si vous avez plusieurs comptes, utilisez le même CFT pour chaque compte.
2. Chargez le CFT dans le portail AWS CloudFormation de chaque compte AWS pour lequel le rôle IAM souhaité existe.

   Vous pouvez appliquer le CFT à l'aide du portail ou de la CLI, comme décrit à l'étape précédente.

   Lorsque vous chargez le CFT, AWS demande ce qui suit :

   1. Nom de la politique (il peut s'agir de n'importe quel nom. Par exemple, connecteur Cisco Secure Workload)
   2. Liste des ARN de compartiment et des ARN d'objet (par défaut : *)

3. Nom du rôle : nom du rôle IAM AWS auquel vous appliquez le CFT
4. Liste des ARN de VPC (par défaut : *)

Étape 8 Cliquez sur **Getting Started guide** (Guide de démarrage, recommandé) ou sur le bouton **Configure your new connector here** (configurer votre nouveau connecteur ici) pour configurer le connecteur.

Étape 9 Comprenez et respectez les Exigences et prérequis AWS, et Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, puis cliquez sur **Get Started** (Démarrer). Ou, si vous effectuez la configuration à l'aide du bouton **Configure your new connector**, (Configurer votre nouveau connecteur) cliquez sur **yes** (oui).

Étape 10 Nommez le connecteur et saisissez la description.

Étape 11 Configurer les paramètres :

Vous pouvez utiliser l'une ou l'autre de ces options pour vous connecter au compte AWS.

1. Clés d'authentification
2. Rôles

Nom du paramètre	Attribut	Description
Clés d'authentification	Access Key	ID de la CLÉ d'accès associé à l'utilisateur AWS qui dispose des privilèges décrits dans le CFT ci-dessus.
	Secret Key	CLÉ SECRÈTE associée à l'ID de la CLÉ D'ACCÈS ci-dessus.
Rôles	Identifiant externe	Il s'agit d'un identifiant unique généré automatiquement pour accorder l'accès aux ressources AWS. Il est utilisé par l'utilisateur pour ajouter une relation de confiance au rôle.
	ARN de l'utilisateur	Il s'agit d'un identifiant unique généré automatiquement attribué à un IAM. Il est utilisé par l'utilisateur pour ajouter une relation de confiance au rôle.
	ARN	Un identifiant unique attribué à chaque ressource AWS.
	HTTP Proxy	(Facultatif) Serveur mandataire requis pour que Cisco Secure Workload atteigne AWS.

Nom du paramètre	Attribut	Description
	Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire d'AWS. La valeur par défaut et minimale est de 3 600 secondes.
	Delta Scan Interval	La fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles apportées aux données d'inventaire auprès d'AWS. La valeur par défaut et minimale est de 600 secondes.

Étape 12 Cliquez sur Next (suivant).

Étape 13 La page suivante affiche une **arborescence des ressources** que l'utilisateur peut développer pour visualiser différentes régions. À l'intérieur de la région, vous pouvez cocher ou décocher les cases des ressources pour obtenir la liste des VPC et des grappes EKS d'AWS.

Étape 14 Dans la liste des réseaux virtuels (VPC), choisissez les VPC pour lesquels vous souhaitez activer les fonctionnalités que vous avez sélectionnées.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

Notez que, comme EKS prend uniquement en charge la capacité de collecte d'étiquettes, aucune sélection de capacité explicite n'a été fournie. La sélection d'une grappe EKS activera implicitement la capacité prise en charge. Pour chaque grappe pour laquelle vous activez cette fonctionnalité, saisissez le **Assume Role ARN** (ARN du rôle assumé) (le numéro de ressource Amazon du rôle à assumer lors de la connexion à Cisco Secure Workload.

Enable Segmentation (activer la segmentation) sur les VPC supprimera le ou les groupes de sécurité existants et fournira un accès par défaut à tous les VPC.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Ultérieurement, lorsque vous serez prêt à appliquer la politique de segmentation pour des VPC spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces VPC. Consultez le document de Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.

Étape 15 Pour la grappe EKS, vous pouvez autoriser l'accès au rôle AWS IAM en fournissant l'ID d'accès Assume Role ARN pour vous connecter au connecteur AWS.

Étape 16 Une fois vos sélections terminées, cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation soit terminée.

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous activez l'acquisition de flux, cela prendre jusqu'à 25 minutes avant que les flux ne commencent à s'afficher dans la page **Investigate** > **Traffic** (Enquêter sur le trafic).

- (Facultatif) Pour approfondir les données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail basées sur VPC. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur AWS pour qu'il recueille les étiquettes et les flux d'acquisition, suivez le processus standard pour créer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier les portées (en général une pour chaque VPC); créer un espace de travail pour chaque portée; découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier que vos politiques respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un VPC particulier, revenez à la configuration du connecteur pour activer la segmentation pour le VPC. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS, à la page 78.

Si vous avez activé l'option des services gérés par Kubernetes (EKS) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez la section *Agents Kubernetes/OpenShift : Visibilité et application approfondies* dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur AWS

Vous pouvez modifier un connecteur AWS, par exemple pour activer l'application de la segmentation pour des VPC spécifiques ou pour apporter d'autres modifications.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procedure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage (Gestion)** > **Workloads(Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **AWS**.

Étape 3 Si vous possédez plusieurs connecteurs AWS, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, consultez Configurer un nouveau connecteur AWS , on page 73.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données EKS), vous devez télécharger le modèle Cloud Formation (CFT) révisé et le téléverser sur AWS avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez satisfait aux conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de

segmentation pour l'inventaire AWS. Sur la page qui répertorie les VPC, choisissez **Enable Segmentation** (activer la segmentation) pour les VPC sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des VPC sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this step** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser) > Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portée pour les VPC sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parentale au-dessus de l'arborescence des portées, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS

Warning Avant d'activer l'application de la segmentation sur un VPC, créez une sauvegarde des groupes de sécurité sur ce VPC. L'activation de la segmentation pour un VPC supprime les groupes de sécurité existants de ce VPC. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité.

Lors de la création de politiques :

- Comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.
- Étant donné qu'AWS n'autorise que les règles ALLLOW (Autoriser) dans les groupes de sécurité, vos politiques de segmentation ne doivent inclure que des politiques Allow, sauf la politique collectrice Catch-All, qui doit avoir l'action Deny (Refuser).

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le VPC associé. Si vous activez la segmentation pour un VPC qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce VPC.

Lorsque vous êtes prêt à appliquer une politique pour un VPC, modifiez le connecteur AWS (voir Modifier un connecteur AWS) et activez la segmentation pour ce VPC.

Afficher les étiquettes d'inventaire, les détails et l'état d'application AWS

Pour afficher des informations résumées sur un connecteur AWS, accédez à la page du connecteur (Manage > Connectors), (Gérer > Connecteurs) puis sélectionnez le connecteur en haut de la page. Pour plus de détails, cliquez sur la ligne d'un VPC.

Pour afficher des informations sur l'inventaire de VPC AWS, cliquez sur une adresse IP dans la page AWS Connectors (Connecteurs AWS) afin d'afficher la page Inventory Profile (Profil d'inventaire) pour cette charge de travail. Pour en savoir plus sur les profils d'inventaire, consultez Profil d'Inventaire.

Pour en savoir plus sur les étiquettes, consultez :

- Étiquettes générées par Cloud Connector

- Étiquettes liées aux grappes Kubernetes

Des politiques concrètes pour l'inventaire VPC sont générées en fonction de leur valeur d'étiquette orchestrator_system/interface_id. Vous pouvez le voir sur la page Inventory Profile (Profil d'inventaire).

Pour afficher l'état d'application, choisissez **Defend (Défendre)** > **Enforcement Status ('État d'application)** dans la barre de navigation à gauche de la fenêtre Cisco Secure Workload. Pour en savoir plus, consultez État d'application pour les connecteurs du nuage.

Résoudre les problèmes de connecteur AWS

Problème : La page Enforcement Status (État de la mise en application) indique qu'une politique concrète a été SKIPPED (IGNORÉE).

Solution : Cette situation se produit lorsque le nombre de groupes de sécurité dépasse les limites d'AWS, telles que configurées dans le connecteur AWS.

Lorsqu'une politique concrète s'affiche comme SKIPPED (IGNORÉE), les nouveaux groupes de sécurité ne sont pas mis en œuvre et les groupes de sécurité existants sur AWS restent en vigueur.

Pour résoudre ce problème, voyez si vous pouvez consolider les politiques, par exemple en utilisant un sous-réseau plus grand dans une politique plutôt que plusieurs avec des sous-réseaux plus petits.

Si vous choisissez d'augmenter les limites du nombre de règles, vous devez communiquer avec Amazon avant de modifier les limites dans la configuration du connecteur AWS.

Contexte :

Des politiques concrètes sont générées pour chaque VPC lorsque la segmentation est activée. Ces politiques concrètes sont utilisées pour créer des groupes de sécurité dans AWS. Cependant, AWS et Cisco Secure Workload comptabilisent les politiques différemment. Lors de la conversion des politiques Cisco Secure Workload en groupes de sécurité AWS, AWS compte chaque sous-réseau unique comme une règle.

Exemple de comptabilisation :

Examinez l'exemple de politique Cisco Secure Workload suivant :

SORTANT : ensemble d'adresses du client -> ensemble d'adresses du fournisseur – Autoriser les ports TCP 80, 8080

AWS compte cette politique comme (le nombre de sous-réseaux uniques dans l'ensemble d'adresses du fournisseur) multiplié par (le nombre de ports uniques).

Ainsi, si l'ensemble d'adresses du fournisseur se compose de 20 sous-réseaux uniques, cette politique Cisco Secure Workload unique compte dans AWS comme 20 (sous-réseaux uniques) * 2 (ports uniques) = 40 règles dans les groupes de sécurité.

Gardez à l'esprit que, comme les VPC sont dynamiques, le nombre de règles l'est également : les nombres sont donc approximatifs.

Problème : AWS autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes s'exécutant sur AWS (EKS)

Si vous avez déployé Amazon Elastic Kubernetes Service (EKS) sur votre nuage AWS, vous pouvez utiliser un connecteur AWS pour extraire l'inventaire et les étiquettes (balises EKS) de votre grappe Kubernetes.

Lorsqu'un connecteur AWS est configuré pour extraire des métadonnées de services Kubernetes gérés, Cisco Secure Workload se connecte au serveur d'API de la grappe et suit l'état des nœuds, des pods et des services de cette grappe. Pour les étiquettes Kubernetes collectées et générées à l'aide de ce connecteur, consultez Étiquettes liées aux grappes Kubernetes.

Exigences et prérequis EKS

- Vérifiez que votre version de Kubernetes est prise en charge. Consultez https://www.cisco.com/go/secure-workload/requirements/integrations.
- Configurer l'accès requis dans EKS, comme décrit ci-dessous.

Rôles et privilèges d'accès EKS

Les informations d'identification de l'utilisateur et l'ARN AssumeRole (le cas échéant) doivent être configurées avec un ensemble minimal de privilèges. L'utilisateur/le rôle doit être spécifié dans la carte de configuration aws-auth.yaml. La carte de configuration aws-auth.yaml peut être modifiée à l'aide de la commande suivante.

```
$ kubectl edit configmap -n kube-system aws-auth
```

Si AssumeRole n'est pas utilisé, l'utilisateur doit être ajouté à la section « mapUsers » de la carte de configuration aws-auth.yaml avec le groupe approprié. Si l'ARN AssumeRole est spécifié, le rôle doit être ajouté à la section « mapRoles » de la carte de configuration aws-auth.yaml. Un exemple de carte de configuration aws-auth.yaml avec AssumeRole est fourni ci-dessous.

```
apiVersion: v1
data:
  mapAccounts: |
    []
  mapRoles: |
    - "groups":
      - "system:bootstrappers"
      - "system:nodes"
     "rolearn": "arn:aws:iam::938996165657:role/eks-cluster-20210114181445234700000000a"

      "username": "system:node:{{EC2PrivateDNSName}}"
    - "rolearn": arn:aws:iam::938996165657:role/BasicPrivilegesRole
      "username": secure.workload.read.only-user
      "groups":
        - secure.workload.read.only

  mapUsers: |
    []
kind: ConfigMap
metadata:
  creationTimestamp: "2021-01-14T18:14:47Z"
  managedFields:
  - apiVersion: v1
    fieldsType: FieldsV1
    fieldsV1:
      f:data:
        .: {}
        f:mapAccounts: {}
        f:mapRoles: {}
        f:mapUsers: {}
    manager: HashiCorp
    operation: Update
    time: "2021-01-14T18:14:47Z"
  name: aws-auth
  namespace: kube-system
```

```
    resourceVersion: "829"
    selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
    uid: 6c5a3ac7-58c7-4c57-a9c9-cad701110569
```

Considérations RBAC spécifiques à EKS

Créer un lien de rôle de grappe entre le rôle de grappe et le compte d'utilisateur/de service.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: csw-clusterrolebinging
subjects:
- kind: User
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
  kubectl create -f clusterrolebinding.yaml
clusterrolebinding.rbac.authorization.k8s.io/csw-clusterrolebinging created
```

Pour en savoir plus sur les rôles et l’accès EKS, consultez la section Rôles EKS et privilèges d’accès.

Configurer les paramètres EKS dans l'assistant du connecteur AWS

Vous activez la fonctionnalité des Services gérés Kubernetes lorsque vous configurez le connecteur AWS. Consultez la section Configurer un nouveau connecteur AWS , on page 73.

Vous aurez besoin de l'ARN Assume Role (ARN Assumer le rôle) pour chaque grappe EKS. Pour en savoir plus, consultez https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html.

Si vous utilisez l’utilisateur AWS pour accéder à la grappe EKS, permettez à l’utilisateur d’accéder à la fonction Assumer le rôle.

Si vous utilisez un rôle IAM entre comptes, permettez au rôle IAM d’accéder à Assumer le rôle.

Prise en charge de l’équilibreur de charge EKS

Nous ajoutons la prise en charge des services de l’équilibreur de charge dans EKS. Les agents Cisco CSW appliquent les règles aux hôtes consommateurs et aux hôtes/pods fournisseurs.

Un équilibreur de charge EKS offre deux options :

1. Conserver l’adresse IP du client.
2. Sur le pod du fournisseur, nous générons
3. Type de cible.

Avant de commencer les scénarios, pour l’intent de politique suivante :

Le service de consommateur à fournisseur, de protocole de service et de port avec des règles d’action Allow (autorisation) pour divers cas est généré comme suit :

Scénario	Conserver l'adresse IP du client	Type de cible
1	Activé	IP
2	Activé	Instance

Scénario	Conserver l'adresse IP du client	Type de cible
3	Désactivé	IP
4	Désactivé	Instance

Cas 1 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Il n'y a pas de règle d'hôte sur le nœud fournisseur, mais nous générons une règle d'entrée sur le pod fournisseur avec la source comme pod consommateur, la destination comme pod de fournisseur (tout), le protocole comme protocole cible, le port comme port cible, et (Allow, autoriser) comme action.

Cas 2 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Le nœud fournisseur génère une règle de préroutage dont la source est le consommateur et la destination tous les nœuds fournisseurs, le protocole le protocole du service, le port le port du nœud du service et l'action l'autorisation.

Sur le pod fournisseur, nous générons une règle d'entrée dont la source est le nœud fournisseur, la destination le pod fournisseur (quelconque), le protocole le protocole cible, le port le port cible et l'action l'autorisation.

Cas 3 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Il n'y a aucune règle d'hôte sur le nœud du fournisseur. Sur le pod fournisseur, nous générons une règle d'entrée avec la source comme ip d'entrée lb, la destination comme pod fournisseur (quelconque), le protocole comme protocole cible, le port comme port cible et l'action comme autorisation.

Cas 4 :

Sur le nœud du consommateur, nous générons une règle de sortie avec le protocole de service du consommateur au service de l'équilibreur de charge (lb ingress ip) et une autorisation de port.

Le nœud fournisseur génère une règle de préroutage qui définit les adresses IP d'entrée comme source et tous les nœuds fournisseurs comme destination. La règle spécifie le protocole du service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod fournisseur, nous générons une règle d'entrée dont la source est le nœud fournisseur, la destination le pod fournisseur (quelconque), le protocole le protocole cible, le port le port cible et l'action l'autorisation.

Connecteur Azure

Le connecteur Azure se connecte à votre compte Microsoft Azure pour effectuer les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses balises) en direct à partir de vos réseaux virtuels Azure (VNets)** Azure vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload peut intégrer les balises associées aux machines virtuelles et aux interfaces réseau, qui peuvent ensuite être utilisées comme étiquettes dans Cisco Secure Workload pour la visualisation des données d'inventaire et des flux de trafic et les définitions de politiques. Ces métadonnées sont synchronisées en permanence.

Les balises des charges de travail et des interfaces réseau de l'abonnement associé au connecteur sont intégrées. Si les charges de travail et les interfaces réseau sont configurées, les balises sont fusionnées et affichées dans Cisco Secure Workload. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques.

- **Acquisition des journaux de flux** Le connecteur peut intégrer les journaux de flux que vous configurez dans Azure pour vos groupes de sécurité réseau (NSG). Vous pouvez ensuite utiliser ces données de télémétrie dans Cisco Secure Workload pour la génération de politiques de visualisation et de segmentation.
- **Segmentation** Lorsque l'application de la politique de segmentation est activée pour un réseau virtuel, les politiques Cisco Secure Workload sont appliquées à l'aide des groupes de sécurité réseau natifs d'Azure.
- **Acquisition automatisée des métadonnées des grappes AKS** Lorsque les services Azure Kubernetes (AKS) sont exécutés sur Azure, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et d'espaces liées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir laquelle des capacités ci-dessus vous souhaitez activer pour chaque réseau virtuel.

Le connecteur Azure prend en charge plusieurs abonnements.

Remarque Les régions de la Chine ne sont actuellement pas prises en charge.

Exigences et prérequis Azure

Pour toutes les fonctionnalités : un seul connecteur peut gérer plusieurs abonnements. Vous aurez besoin d'un ID d'abonnement pour configurer le connecteur. Cet ID d'abonnement peut être l'un des nombreux ID d'abonnement qui sont intégrés à un connecteur.

Dans Azure, créer et enregistrer une application à l'aide d'Azure Active Directory (AD). Vous aurez besoin des renseignements suivants provenant de cette application :

- ID (client) d'application
- ID de l'annuaire (détenteur)
- Renseignements d'authentification client (vous pouvez utiliser un certificat ou une clé secrète client)
- Identifiant d'abonnement

L'assistant de configuration du connecteur génère un modèle de gestionnaire de ressources Azure (ARM) que vous pouvez utiliser pour créer un rôle personnalisé avec les autorisations nécessaires pour les fonctionnalités du connecteur que vous choisissez d'activer. Ces autorisations s'appliqueront à toutes les ressources de l'abonnement que vous spécifiez pour le connecteur. Assurez-vous que vous disposez des autorisations dans Azure pour charger ce modèle.

Si la connectivité l'exige, assurez-vous qu'un serveur mandataire HTTP est disponible pour cette intégration.

Chaque réseau virtuel (VNet) ne peut appartenir qu'à un seul connecteur Azure. Un compte Azure peut avoir plusieurs connecteurs Azure.

Ce connecteur ne nécessite pas d'appliance virtuelle.

Pour la collecte d'étiquettes et de l'inventaire : aucune condition préalable supplémentaire n'est requise.

Pour l'acquisition des journaux de flux : chaque réseau virtuel (VNet) doit avoir au moins un sous-réseau configuré.

Chaque sous-réseau de chaque réseau virtuel doit être associé à un groupe de sécurité réseau (NSG). Vous pouvez associer un seul NSG à plusieurs sous-réseaux. Vous pouvez définir n'importe quel groupe de ressources lors de la configuration du groupe de sécurité réseau.

Seul le trafic qui atteint une règle NSG sera inclus dans les journaux de flux. Par conséquent, chaque groupe de sécurité réseau devrait avoir au moins une règle pour le trafic entrant et une règle pour le trafic sortant qui s'applique à n'importe quelle source et à toute destination. L'équivalent d'une règle collectrice globale dans Cisco Secure Workload. (Par défaut, les groupes de sécurité réseau incluent ces règles).

Les journaux de flux doivent être activés pour chaque groupe de sécurité réseau.

- Un compte de stockage dans Azure est requis. Des autorisations d'accès doivent être incluses pour l'abonnement que vous utilisez pour ce connecteur.
- Les journaux de flux doivent utiliser la version 2.
- La durée de conservation peut être de deux jours (le connecteur extrait de nouvelles données de flux toutes les minutes, et deux jours devraient laisser suffisamment de temps pour résoudre les échecs de connexion).

Pour la segmentation : l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Lorsque vous activez la segmentation pour un réseau virtuel (VNet), toutes les règles existantes sont supprimées des groupes de sécurité réseau associés aux sous-réseaux et aux interfaces réseau qui font partie de ces sous-réseaux. Sauvegardez vos règles existantes de groupe de sécurité réseau du sous-réseau et de l'interface réseau avant d'activer la segmentation dans le connecteur.

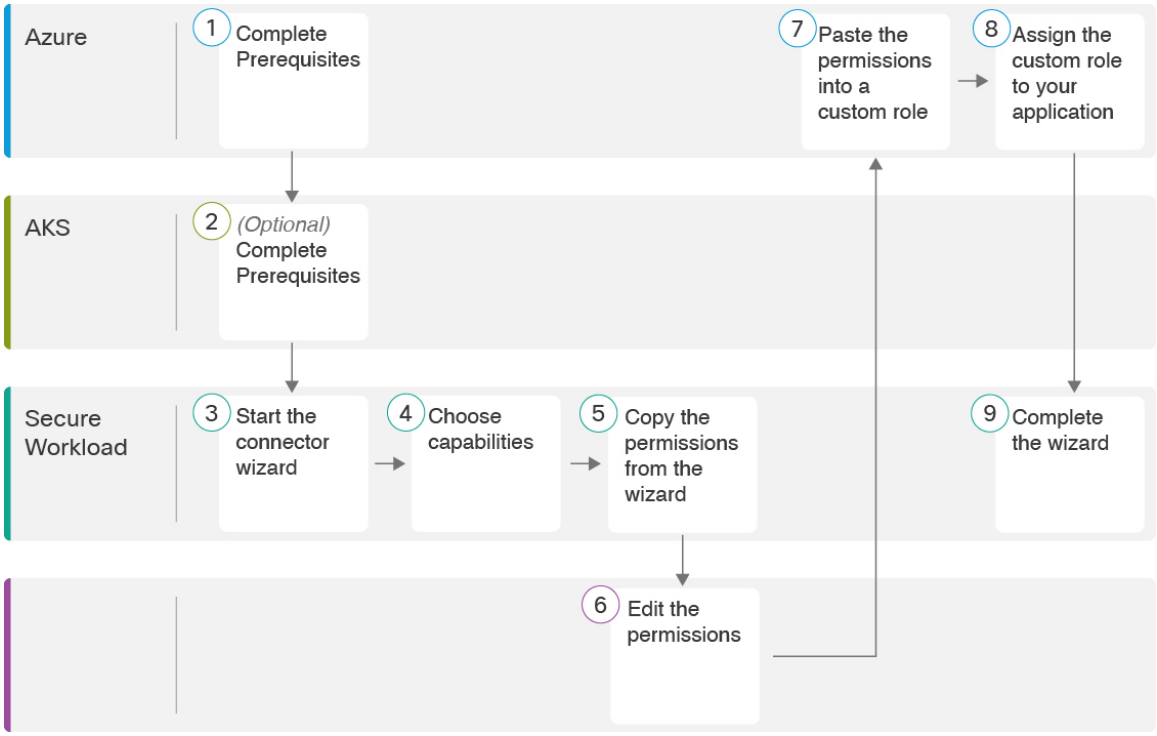
Voir également Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 89, ci-dessous.

Pour les services Kubernetes gérés (AKS) : si vous activez l'option Kubernetes AKS, consultez les exigences et les conditions préalables dans la section des services Kubernetes gérés fonctionnant sur Azure (AKS) ci-dessous, .

Présentation de la configuration du connecteur Azure

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour en savoir plus sur les renseignements importants, consultez la rubrique suivante (Configurer un connecteur Azure).

Illustration 43 : Présentation de la configuration du connecteur Azure



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un connecteur Azure

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur le connecteur Azure.

Étape 3 Cliquez sur **Enable** (activer) pour le premier connecteur (dans une portée racine) ou **Enable Another** (activer un autre connecteur) pour les connecteurs supplémentaires de la même portée racine.

Étape 4 Comprenez et respectez les exigences et les prérequis dans le document Exigences et prérequis Azure, puis cliquez sur Get Started (Démarrer).

Étape 5 Nommez le connecteur et choisissez les fonctionnalités souhaitées :

Les sélections que vous effectuez sur cette page sont utilisées uniquement pour déterminer les privilèges inclus dans le modèle de gestionnaire de ressources Azure (ARM) qui sera généré à l'étape suivante et pour afficher les paramètres que vous devrez configurer.

Pour activer la segmentation, vous devez également activer **Gather Labels** (Regrouper les étiquettes).

L'activation de la segmentation sur cette page ne permet pas en elle-même l'application des politiques et n'affecte pas les groupes de sécurité réseau existants. L'application des politiques et la suppression des groupes de sécurité existants se produisent uniquement si vous activez la segmentation pour les réseaux virtuels ultérieurement dans l'assistant. Vous pouvez revenir à cet assistant plus tard pour activer l'application de la politique de segmentation pour les réseaux virtuels individuels.

Étape 6 Cliquez sur **Next** (suivant) et lisez les informations sur la page de configuration.

Étape 7 Votre abonnement doit disposer des privilèges requis pour que vous puissiez passer à la page suivante de l'assistant.

Pour utiliser le modèle Azure Resource Manager (ARM) fourni pour attribuer les autorisations requises pour le connecteur :

1. Téléchargez le modèle ARM à partir de l'assistant.
2. Modifiez le texte du modèle pour remplacer **<subscription_ID>** par votre numéro d'abonnement.

   Remarque Pour un connecteur, vous pouvez créer plusieurs ID d'abonnement dans le compte Azure.

   Vous pouvez saisir plusieurs ID d'abonnement lorsque les informations d'authentification appartiennent au même ID d'abonnement.

3. Dans Azure, créez un rôle personnalisé dans l'abonnement applicable.
4. Dans le formulaire de rôle personnalisé, pour les autorisations de référence, choisissez **Start from zero** (Démarrer à partir de zéro).
5. Dans l'onglet JSON du formulaire de création de rôle personnalisé, collez le texte du fichier modifié que vous avez téléchargé à partir de l'assistant de connecteur.
6. Enregistrez le rôle personnalisé.
7. Associez le rôle personnalisé à l'application que vous avez configurée dans les conditions préalables pour cette procédure.

Ce modèle dispose des autorisations IAM requises pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option des services gérés par Kubernetes, vous devez configurer séparément les autorisations pour AKS. Consultez Services gérés Kubernetes fonctionnant sur Azure (AKS), à la page 90.

Étape 8 Configurer les paramètres :

Attribut	Description
SubscriptionID	ID de l'abonnement Azure que vous associez à ce connecteur.
ClientID	**ID d'application (client)** de l'application que vous avez créée dans Azure pour ce connecteur.
TenantID	L' **ID de l'annuaire (détenteur)** de l'application que vous avez créée dans Azure pour ce connecteur.
Clé secrète du client ou certificat du client	Pour l'authentification, vous pouvez utiliser une clé secrète client ou un certificat client et une clé. Obtenez l'un ou l'autre à partir du lien **Informations d'identification client** dans l'application que vous avez créée dans Azure pour ce connecteur. Si vous utilisez un certificat : le certificat doit être non chiffré. Seuls les certificats RSA sont pris en charge Les clés privées peuvent être PKCS1 ou PKCS8.

Attribut	Description
HTTP Proxy	Serveur mandataire requis pour que Cisco Secure Workload atteigne Azure. Ports serveur mandataire pris en charge : 80, 8080, 443 et 3128.
Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire d'Azure. La valeur par défaut et minimale est de 3 600 secondes.
Delta Scan Interval	Fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles des données d'inventaire auprès d'Azure. La valeur par défaut et minimale est de 600 secondes.

Étape 9 Cliquez sur **Next** (suivant). Le système peut nécessiter quelques minutes pour obtenir la liste des réseaux virtuels et des grappes AKS d'Azure.

Étape 10 Dans la liste des réseaux virtuels et des grappes AKS pour chaque réseau virtuel, choisissez les réseaux virtuels et les grappes AKS pour lesquels vous voulez activer les fonctionnalités sélectionnées.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

Notez que, puisqu'AKS prend uniquement en charge la capacité de collecte d'étiquettes, aucune sélection de capacité explicite n'a été fournie. La sélection d'une grappe AKS activera implicitement la capacité prise en charge. Téléversez le certificat client et la clé pour chaque grappe pour laquelle vous activez cette fonctionnalité.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Plus tard, lorsque vous serez prêt à appliquer la politique de segmentation pour des réseaux virtuels spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces réseaux. Consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 89.

Étape 11 Une fois vos sélections terminées, cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation soit terminée.

La page View Groups (Afficher les groupes) affiche tous les réseaux virtuels que vous avez activés pour les fonctionnalités de la page précédente, regroupés par région. Chaque région et chaque réseau virtuel dans chaque région constitue une nouvelle portée.

Étape 12 (Facultatif) Choisissez la portée parente sous laquelle ajouter le nouvel ensemble de portées. Si vous n'avez encore défini aucune portée, votre seule possibilité est la portée par défaut.

Étape 13 (Facultatif) Pour accepter tous les paramètres configurés dans l'assistant, *y compris* l'arborescence de portée hiérarchique, cliquez sur **Save**(enregistrer) .

Pour accepter tous les paramètres à l'*exception* de l'arborescence de la portée hiérarchique, cliquez sur **Skip** (Ignorer) cette étape.

Vous pourrez créer ou modifier manuellement l'arborescence de la porte ultérieurement, sous **Organiser (Organiser)** > **Scopes and Inventory (Portées et inventaires**).

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous avez activé l'acquisition de flux, 25 minutes peuvent être nécessaires avant que les flux ne commencent à s'afficher sur la page **Investigate (Enquêter)** > **Traffic (Trafic)** .
- (Facultatif) Pour approfondir des données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail de réseau virtuel. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur Azure pour recueillir des étiquettes et des flux d'acquisition, suivez le processus standard pour créer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier la portée (en général une pour chaque réseau virtuel); créer un espace de travail pour chaque portée; découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier qu'elles respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un réseau virtuel donné, revenez à la configuration du connecteur pour activer la segmentation pour ce réseau virtuel. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 89.

Si vous avez activé l'option des services gérés par Kubernetes (AKS) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez Installer les agents Kubernetes ou OpenShift pour une visibilité et une application approfondies dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur Azure

Vous pouvez modifier un connecteur Azure, par exemple pour activer l'application de la segmentation pour des réseaux virtuels spécifiques ou pour apporter d'autres modifications.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur **Azure**.

Étape 3 Si vous avez plusieurs connecteurs Azure, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, reportez-vous à Configurer un connecteur Azure, à la page 85.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données AKS), vous devez télécharger le modèle ARM révisé, modifier le texte du nouveau modèle pour préciser l'ID d'abonnement, et charger le nouveau modèle dans le rôle personnalisé que vous voulez. créé dans Azure avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez rempli les conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure, à la page 89. Ensuite, sur la page de l'assistant qui répertorie les réseaux virtuels, choisissez **Enable Segmentation** (activer la segmentation) pour les réseaux virtuels sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des réseaux virtuels sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this étape** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser) > Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portées pour les réseaux virtuels sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parente dans la partie supérieure de l'arborescence, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure

Avertissement Avant d'activer l'application de la segmentation sur un réseau virtuel, créez une sauvegarde des groupes de sécurité réseau sur ce réseau virtuel. L'activation de la segmentation pour un réseau virtuel supprime les règles existantes du groupe de sécurité réseau associé à ce dernier. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité réseau.

Lors de la création de politiques : comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le réseau virtuel associé. Si vous activez la segmentation pour un réseau virtuel qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce réseau virtuel.

Lorsque vous êtes prêt à appliquer la politique pour un réseau virtuel, modifiez le connecteur Azure (voir Modifier un connecteur Azure, à la page 88) et activez la segmentation pour ce réseau virtuel.

Notez que si un sous-réseau n'est associé à aucun groupe de sécurité de réseau, Cisco Secure Workload n'applique pas la politique de segmentation sur ce sous-réseau. Lorsque vous appliquez la politique de segmentation sur un réseau virtuel, le groupe de sécurité réseau au niveau du sous-réseau est modifié pour autoriser tout le trafic, et les politiques Cisco Secure Workload remplacent le groupe de sécurité réseau au niveau de l'interface. Un groupe de sécurité réseau pour l'interface est automatiquement créé s'il n'est pas déjà présent.

Afficher les étiquettes d'inventaire, les détails et l'état d'application d'Azure

Pour afficher des renseignements résumés sur un connecteur Azure, accédez à la page du connecteur (Manage > Connectors) (Gérer > Connecteurs), puis sélectionnez le connecteur en haut de la page. Pour plus de détails, cliquez sur une ligne VNet.

Pour afficher des informations sur l'inventaire VNet Azure, cliquez sur une adresse IP dans la page Azure Connectors (connecteurs Azure) afin d'afficher la page Inventory Profile (Profil d'inventaire) pour cette charge de travail. Pour en savoir plus sur les profils d'inventaire, consultez Profil d'Inventaire.

Pour en savoir plus sur les étiquettes, consultez :

- Étiquettes générées par les connecteurs infonuagiques
- Étiquettes liées aux grappes Kubernetes

Des politiques concrètes pour l'inventaire de réseau virtuel sont générées en fonction de leur valeur d'étiquette orchestrator_system/interface_id. Vous pouvez le voir sur la page Inventory Profile (Profil d'inventaire).

Pour afficher l'état d'application, choisissez **Defend (Défendre)** > **Enforcement Status ('État d'application)** dans la barre de navigation à gauche de la fenêtre Cisco Secure Workload. Pour en savoir plus, consultez État d'application pour les connecteurs du nuage.

Résoudre les problèmes de connecteur Azure

Problème : Azure autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes fonctionnant sur Azure (AKS)

Si vous avez déployé Azure Kubernetes Services (AKS) sur votre nuage Azure, vous pouvez utiliser un connecteur Azure pour extraire dynamiquement l'inventaire et les étiquettes (balises AKS) de votre grappe Kubernetes.

Lorsqu'un connecteur Azure est configuré pour extraire des métadonnées de services Kubernetes gérés, Cisco Secure Workload suit l'état des nœuds, des pods et des services de cette grappe.

Pour les étiquettes Kubernetes collectées et générées à l'aide de ce connecteur, consultez Étiquettes liées aux grappes Kubernetes.

Requirements and Prerequisites for AKS

- Verify that your Kubernetes version is supported. See the Compatibility Matrix for the operating systems, external systems, and connectors for Secure Workload agents.
- Enable and configure the Managed Kubernetes Services (AKS) capability when you configure the Azure connector. See Configurer un connecteur Azure for details.

Prise en charge de l'équilibreur de charge AKS

AKS prend en charge la conservation de l'adresse IP du client.

Pour l'intent de politique suivant :

Le service de consommateur à fournisseur, le protocole de service et le port avec des règles d'action Allow (autorisation) dans différents scénarios se génèrent comme suit :

Scénario	Conserver l'adresse IP du client
1	Activé
2	Désactivé

Scénario 1 : la fonction Conserver l'adresse IP du client est **activée**.

Sur le nœud du consommateur, nous générons une règle de sortie avec le service du consommateur vers l'équilibreur de charge (lb ingress ip), le protocole du service et le port sont autorisés.

Une règle de préroutage générée pour le nœud fournisseur, qui définit le consommateur comme source et tous les nœuds fournisseurs comme destination. La règle inclut le protocole de service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod du fournisseur, nous générons une règle d'entrée avec source comme nœuds de fournisseur, une destination comme pod de fournisseur (n'importe lequel), le protocole comme protocole cible, le port comme port cible et l'action comme allow (autoriser).

Scénario 2 : la fonction de conservation de l'adresse IP du client est **désactivée**.

Sur le nœud du consommateur, nous générons une règle de sortie avec le service du consommateur vers l'équilibreur de charge (lb ingress ip), le protocole du service et le port sont autorisés.

Le nœud fournisseur génère une règle de préroutage qui définit les adresses IP d'entrée comme source et tous les nœuds fournisseurs comme destination. La règle spécifie le protocole du service comme protocole et le port de nœud du service comme port, avec l'action définie sur allow (autoriser).

Sur le pod du fournisseur, nous générons une règle d'entrée avec la source comme nœuds de fournisseur, la destination comme pod de fournisseur (n'importe quel), le protocole comme protocole cible, le port comme port cible et l'action comme allow (autoriser).

Connecteur GCP

Le connecteur Google Cloud Platform se connecte à GCP pour effectuer les fonctions générales suivantes :

- **Acquisition automatisée de l'inventaire (et de ses balises) en direct à partir du nuage privé virtuel (VPC) GCP**

  GCP vous permet d'affecter des métadonnées à vos ressources sous forme de balises. Cisco Secure Workload interrogera les balises de ces ressources, qui peuvent ensuite être utilisées pour la visualisation des données d'inventaire et des flux de trafic, et pour la définition de politiques. Cette fonctionnalité maintient le mappage des balises de ressources à jour en synchronisant constamment ces données.

  Les balises des charges de travail et des interfaces réseau d'un VPC GCP sont intégrées. Si les charges de travail et les interfaces réseau sont configurées, les balises sont fusionnées et affichées dans Cisco Secure Workload. Pour en savoir plus, consultez Étiquettes générées par les connecteurs infonuagiques.

- **Acquisition des journaux de flux du VPC** si vous avez configuré les journaux de flux VPC dans GCP à des fins de surveillance, Cisco Secure Workload peut procéder à l'acquisition des informations des journaux de flux en lisant le compartiment de stockage Google correspondant. Ces données de télémétrie peuvent être utilisées pour la génération de politiques de visualisation et de segmentation.

- **Segmentation** : l'activation de cette option permettra à Cisco Secure Workload de programmer les politiques de sécurité à l'aide du pare-feu VPC natif de GCP. Lorsque l'application est activée pour un VPC, les politiques pertinentes sont automatiquement programmées sur le pare-feu de celui-ci.

- **Acquisition automatisée des métadonnées des grappes GKE** (capacités K8s) lorsque Google Kubernetes Engine (GKE) s'exécute sur GCP, vous pouvez choisir de rassembler toutes les métadonnées de nœuds, de services et de pods associées à toutes les grappes Kubernetes sélectionnées.

Vous pouvez choisir laquelle des capacités ci-dessus vous souhaitez activer pour chaque VPC.

Exigences et conditions préalables des connecteurs GCP

Pour toutes les fonctionnalités : créez un compte de service dédié dans GCP ou identifiez un compte de service GCP existant pour ce connecteur. L'assistant de configuration du connecteur génère une liste de politiques IAM que vous pouvez utiliser pour attribuer les privilèges requis à ce compte de service. Assurez-vous que vous avez les autorisations dans GCP pour charger cette liste de politiques IAM.

Remarque La méthode recommandée pour appliquer l'autorisation de la liste de politiques IAM au compte de service consiste à utiliser la CLI.

Chaque VPC ne peut appartenir qu'à un seul connecteur GCP. Une grappe Cisco Secure Workload peut avoir plusieurs connecteurs GCP. Recueillez les informations décrites dans les tableaux Configurer un connecteur GCP, à la page 94, ci-dessous.

Ce connecteur ne nécessite pas d'appliance virtuelle.

- **Pour la collecte d'étiquettes et de l'inventaire :** aucune condition préalable supplémentaire n'est requise.
- **Pour l'acquisition des journaux de flux :** des définitions de journaux de flux au niveau VPC sont requises pour déclencher la collecte des journaux de flux.

  Pour utiliser l'acquisition des journaux de flux, l'utilisateur doit activer les journaux de flux sur les VPC souhaités et configurer un récepteur de routeur de journaux.

  Filtre d'inclusion pour le récepteur du routeur de journal :

  1. `resource.type="gce-subnetwork"`
  2. `log_name="projects/<project_id>/logs/compute.googleapis.com%2Fvpc_flows"`

  Choisissez la destination du récepteur en tant que compartiment de stockage infonuagique, puis choisissez l'ensemble de stockage souhaité.

  Lors de la configuration du connecteur GCP avec les journaux de flux d'entrée, il est obligatoire de saisir le nom du compartiment de stockage.

  Seuls les journaux de flux du VPC peuvent être intégrés.

  Les journaux de flux doivent être publiés dans le compartiment de stockage Google; Cisco Secure Workload ne peut pas collecter les données de flux de Google Cloud Operations Suite.

  Cisco Secure Workload peut acquérir des logs de flux à partir d'un compartiment de stockage Google associé à n'importe quel compte, si le compte utilisateur GCP fourni lors de la création du connecteur a accès à la fois aux journaux de flux VPC et au compartiment de stockage Google.

  Les attributs de journal de flux suivants (dans n'importe quel ordre) sont requis dans ce dernier : adresse source, adresse de destination, port source, port de destination, protocole, paquets, octets, heure de début, heure de fin, action, indicateurs TCP, ID d'interface, État du journal et direction du flux. Tout autre attribut est ignoré.

  Les journaux de flux doivent saisir le trafic autorisé et refusé.

- **Pour la segmentation :** l'activation de la segmentation nécessite l'activation de l'option Gather Labels (Rassembler les étiquettes).

Sauvegardez vos groupes de sécurité existants avant d'activer la segmentation dans le connecteur, car toutes les règles existantes seront remplacées lorsque vous activerez l'application de la politique de segmentation pour un VPC.

Voir également Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 98, ci-dessous.

- **Pour les services Kubernetes gérés (GKE) :** si vous activez l'option Kubernetes, consultez les exigences et les conditions préalables dans la section Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 99 ci-dessous, y compris les privilèges d'accès requis.

Configurer l'accès à plusieurs projets dans GCP

Pour configurer l'accès entre plusieurs projets dans GCP, vous pouvez suivre ces étapes :

Procédure

Étape 1 Connectez-vous à votre console GCP.

Étape 2 Cliquez sur le menu déroulant du projet dans la barre de navigation supérieure et sélectionnez **New Project** (Nouveau projet). Vous pouvez soit créer un nouveau projet, soit utiliser un projet existant avec le compte de service.

Étape 3 Saisissez un nom pour votre nouveau projet. Choisissez l'organisation à laquelle appartient le nouveau projet ou sélectionnez **No organization** (Aucune organisation) si vous n'en avez pas.

Étape 4 Cliquez sur le bouton **Create** (Créer) pour créer le nouveau projet.

Remarque Vous pouvez répéter les étapes 2 à 4 pour créer autant de projets que nécessaire.

Étape 5 Pour lier plusieurs projets à un seul compte de service, accédez à la page **IAM & Admin** et choisissez **Service Account** (Compte de service).

Étape 6 Cliquez sur le bouton **Create Service Account** (Créer un compte de service). Suivez les instructions pour créer le compte de service et lui accorder les autorisations nécessaires.

Remarque Vous pouvez soit utiliser un compte de service existant, soit créer un nouveau compte de service.

Étape 7 Sous l'onglet **Keys** (clés), cliquez sur **Add Key** (Ajouter une clé) pour générer une clé privée dans un fichier JSON.

Étape 8 Rendez-vous sur la page **IAM & Admin** de la console GCP et sélectionnez **IAM**.

Remarque Vous devez d'abord changer de projet avant de cliquer sur IAM & Admin, puis essayer d'accorder des privilèges.

Étape 9 Cliquez sur le bouton **Grant access** (accorder l'accès) pour ajouter un nouveau projet.

Étape 10 Dans le champ **New principals** (oNuveaux principaux), saisissez l'adresse courriel du compte de service que vous souhaitez associer au projet.

Étape 11 Cliquez sur le bouton **Save** (Enregistrer) pour associer le compte de service à votre projet.

Remarque Répétez ces étapes pour chaque projet que vous souhaitez lier à votre projet d'origine.

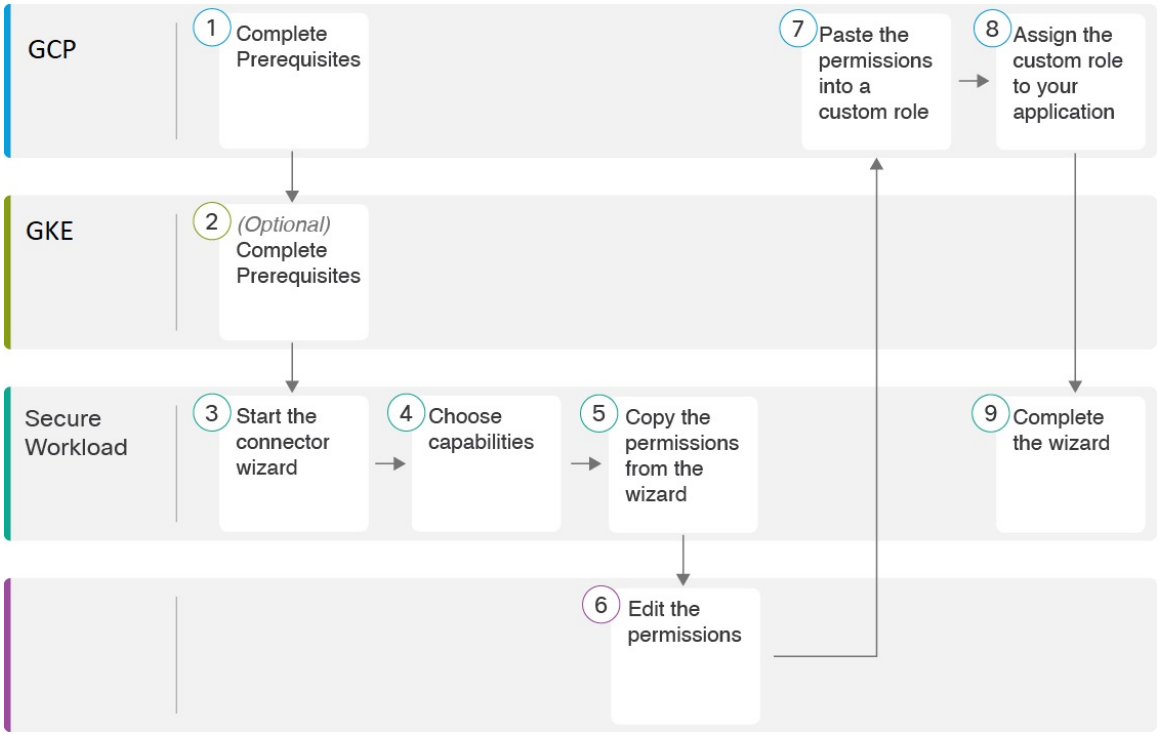
Vous pouvez gérer les autorisations du compte de service en vous rendant sur la page **IAM & Admin** de la console GCP et en sélectionnant **IAM** pour chaque projet.

Étape 12 Assurez-vous que le compte de service dispose d'autorisations pour le niveau de ressources ancêtre le moins élevé commun (ancêtre commun à tous les projets sélectionnés), tel qu'un dossier ou une organisation.

Aperçu de la configuration du connecteur GCP

Le graphique suivant donne un aperçu général du processus de configuration du connecteur. Pour en apprendre davantage, consultez la rubrique suivante (Configurer un connecteur GCP, à la page 94).

Illustration 44 : Aperçu de la configuration du connecteur GCP



(Notez que les numéros dans le graphique ne correspondent pas aux numéros d'étape de la procédure détaillée).

Configurer un connecteur GCP

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage** > **Connectors**(gestion des connecteurs).

Étape 2 Cliquez sur le **GCP connector** (connecteur GCP).

Étape 3 Cliquez sur **Enable** (activer) pour le premier connecteur (dans une portée racine) ou **Enable Another** (activer un autre connecteur) pour les connecteurs supplémentaires de la même portée racine.

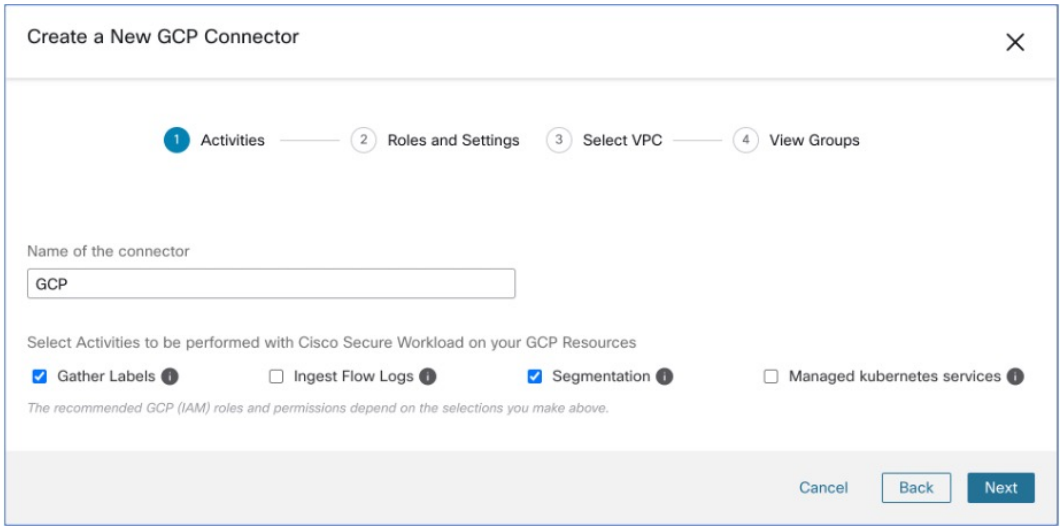
Étape 4 Comprenez et respectez les exigences et les conditions préalables indiquées dans Exigences et conditions préalables des connecteurs GCP, à la page 92 et Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 99, puis cliquez sur **Get Started** (Démarrer).

Étape 5 Attribuez un nom au connecteur et choisissez les fonctionnalités souhaitées, puis cliquez sur **Next** (Suivant).

Les sélections effectuées sur cette page servent uniquement à déterminer les privilèges inclus dans la liste de règles IAM qui sera générée à l'étape suivante, et à afficher les paramètres que vous devrez configurer.

Si la fonctionnalité **Injest Flow Logs** (injecter les journaux de flux) est cochée, vous devez saisir **le nom du compartiment de stockage des journaux** de flux à l'étape suivante.

Pour activer la **segmentation**, vous devez cocher **Gather Labels** (recueillir les étiquettes).



Étape 6 Téléchargez la liste des politiques de rôle personnalisé IAM générée.

Cette liste de politiques de rôles personnalisés IAM dispose des privilèges IAM requis pour les fonctionnalités que vous avez sélectionnées à l'étape précédente.

Si vous avez activé l'option Kubernetes, vous devez configurer séparément les autorisations pour GKE.

Pour en savoir plus, consultez Services gérés Kubernetes s'exécutant sur GCP (GKE), à la page 99.

Étape 7 Chargez le fichier `json du compte de service` avec les fonctionnalités requises qui a été créé comme condition préalable.

Remarque Dans GCP, le connecteur unique prend en charge plusieurs projets et garantit que le compte de service est directement associé à tous les projets.

Étape 8 Saisissez le **nom de la compartiment de stockage des journaux de flux** si la fonctionnalité des journaux de flux d'entrée est cochée.

Étape 9 Configurez les paramètres suivants :

Attribut	Description
HTTP Proxy	serveur mandataire requis pour que Cisco Secure Workload atteigne GCP.
Full Scan Interval	Fréquence à laquelle Cisco Secure Workload actualise les données complètes d'inventaire de GCP. La valeur par défaut et minimale est de 3 600 secondes.

Attribut	Description
Delta Scan Interval	Fréquence à laquelle Cisco Secure Workload récupère les modifications incrémentielles apportées aux données d'inventaire à partir de GCP. La valeur par défaut et minimale est de 600 secondes.

Étape 10 Cliquez sur **Next** (suivant). Quelques minutes peuvent être nécessaires pour que le système obtienne la liste des réseaux virtuels et des grappes GKE de votre (vos) projet(s) GCP.

Étape 11 Dans la liste des VPC (réseaux virtuels) et des grappes GKE, choisissez les ressources et leurs capacités respectives.

En général, vous devez activer l'acquisition de flux dès que possible, afin que Cisco Secure Workload puisse commencer à collecter suffisamment de données pour proposer des politiques précises.

En général, vous ne devez pas choisir **Enable Segmentation** (activer la segmentation) lors de la configuration initiale. Ultérieurement, lorsque vous serez prêt à appliquer la politique de segmentation pour des VPC spécifiques, vous pourrez modifier le connecteur et activer la segmentation pour ces VPC. Consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour un inventaire GCP.

Étape 12 Cliquez sur **Create** (créer) et attendez quelques minutes que la vérification de validation se termine.

La page View Groups (Afficher les groupes) affiche tous les VPC que vous avez activés pour toutes les fonctionnalités sur la page précédente, regroupés par logic_group_id (CSW), qui est également un ID de projet (GCP). Chaque logic_group_id et chaque VPC de chaque logic_group_id est une nouvelle portée.

Étape 13 Choisissez la portée parente sous laquelle ajouter le nouvel ensemble de portées. Si vous n'avez encore défini aucune portée, votre seule possibilité est la portée par défaut.

Étape 14 Pour accepter tous les paramètres configurés dans l'assistant, *y compris* l'arborescence de portée hiérarchique, cliquez sur **Save**(enregistrer).

Pour accepter tous les paramètres à l'*exception* de l'arborescence de la portée hiérarchique, cliquez sur **Skip** (Ignorer) cette étape.

Vous pourrez créer ou modifier manuellement l'arborescence de la porte ultérieurement, sous **Organiser (Organiser)** > **Scopes and Inventory (Portées et inventaires**).

Prochaine étape

Si vous avez activé la collecte d'étiquettes, l'acquisition de données de flux ou la segmentation :

- Si vous avez activé l'acquisition de flux, 25 minutes peuvent être nécessaires avant que les flux ne commencent à s'afficher sur la page **Investigate (Enquêter)** > **Traffic (Trafic)** .
- (Facultatif) Pour approfondir les données de flux et d'autres avantages, notamment une visibilité sur les vulnérabilités de l'hôte (CVE), installez l'agent approprié pour votre système d'exploitation sur vos charges de travail basées sur VPC. Pour connaître les exigences et en savoir plus, consultez le chapitre sur l'installation de l'agent.
- Après avoir configuré avec succès le connecteur GCP pour recueillir des étiquettes et des flux d'acquisition, suivez le processus standard pour élaborer des politiques de segmentation. Par exemple : autorisez Cisco Secure Workload à recueillir suffisamment de données de flux pour générer des politiques fiables; définir ou modifier les portées (en général une pour chaque VPC); créer un espace de travail pour chaque portée;

découvrir automatiquement les politiques en fonction de vos données de flux ou créer manuellement des politiques; analyser et affiner vos politiques; vérifier que vos politiques respectent les directives et les bonnes pratiques ci-dessous; puis, lorsque vous êtes prêt, approuvez et appliquez ces politiques dans l'espace de travail. Lorsque vous êtes prêt à appliquer la politique de segmentation pour un VPC particulier, revenez à la configuration du connecteur pour activer la segmentation pour le VPC. Pour de plus amples renseignements, consultez la section Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 98.

Si vous avez activé l'option des services gérés par Kubernetes (GKE) :

- Installez les agents Kubernetes sur vos charges de travail basées sur des conteneurs. Pour en savoir plus, consultez la section Agents Kubernetes/OpenShift : Visibilité et application approfondies dans le chapitre sur le déploiement des agents.

Journal des événements

Les journaux des événements peuvent être utilisés pour connaître les événements importants qui se produisent par connecteur à partir de différentes capacités. Nous pouvons les filtrer à l'aide de divers attributs tels que le composant, l'espace de nom, les messages et l'horodatage.

Modifier un connecteur GCP

Si vous souhaitez activer la collecte de données à partir de grappes GKE ou de VPC différents ou supplémentaires, vous devrez peut-être charger un fichier json de compte de service avec les fonctionnalités requises et des autorisations différentes avant de pouvoir sélectionner différents VPC ou GKE.

Les modifications ne sont pas enregistrées tant que vous n'avez pas achevé l'exécution de l'assistant.

Procédure

Étape 1 Dans la barre de navigation à gauche de la fenêtre, choisissez **Manage (Gestion)** > **Workloads(Charges de travail)** > **Connectors (Connecteurs)**.

Étape 2 Cliquez sur **GCP connector** (connecteur GCP).

Étape 3 Si vous avez plusieurs connecteurs GCP, choisissez le connecteur à modifier en haut de la fenêtre.

Étape 4 Cliquez sur **Edit Connector** (modifier un connecteur).

Étape 5 Cliquez à nouveau dans l'assistant et apportez des modifications. Pour une description détaillée des paramètres, reportez-vous à Configurer un connecteur GCP, à la page 94.

Étape 6 Si vous activez différentes fonctionnalités (collecte d'étiquettes, acquisition de flux, application de la segmentation ou collecte de données GKE), vous devez télécharger le modèle IAM révisé et le charger dans GKE avant de poursuivre l'assistant.

Étape 7 Pour activer l'application de la politique de segmentation, assurez-vous d'abord que vous avez rempli les conditions préalables recommandées décrites dans Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP, à la page 98. Dans la page qui répertorie les VPC, sélectionnez **Enable Segmentation** (activer la segmentation) pour les VPC sur lesquels vous souhaitez activer l'application.

Étape 8 Si vous avez déjà créé des portées pour l'un des VPC sélectionnés, soit à l'aide de l'assistant, soit manuellement, cliquez sur **Skip this step** (Ignorer cette étape) pour fermer l'assistant.

Vous pouvez modifier l'arborescence de la portée manuellement à l'aide de la page **Organize (Organiser)** > **Scopes and inventory (Portées et inventaire)**.

Étape 9 Si vous n'avez pas encore créé de portée pour les VPC sélectionnés et que vous souhaitez conserver la hiérarchie proposée, choisissez la portée parentale au-dessus de l'arborescence des portées, puis cliquez sur **Save** (Enregistrer).

Suppression des connecteurs et des données GCP

Si vous supprimez un connecteur, les données déjà acquises par ce connecteur ne sont pas supprimées.

Les étiquettes et l'inventaire sont automatiquement supprimés de l'inventaire actif après 24 heures.

Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP

Avertissement Avant d'activer l'application de la segmentation sur un VPC, créez une sauvegarde des groupes de sécurité sur ce VPC. L'activation de la segmentation pour un VPC supprime les groupes de sécurité existants de ce VPC. La désactivation de la segmentation ne restaure pas les anciens groupes de sécurité.

Lors de la création de politiques :

- Comme pour toutes les politiques découvertes, vérifiez que vous disposez de suffisamment de données de flux pour produire des politiques précises.
- Parce que GCP autorise les deux règles ALLOW/DENY (AUTORISER/REFUSER) dans la politique de pare-feu. Depuis, GCP a une limitation très stricte sur le nombre de règles. Donc, il est préférable d'avoir uniquement la liste ALLOW.

Nous vous recommandons d'activer l'application dans l'espace de travail avant d'activer la segmentation pour le VPC associé. Si vous activez la segmentation pour un VPC qui n'est pas inclus dans un espace de travail dont l'application est activée, tout le trafic sera autorisé sur ce VPC.

Lorsque vous êtes prêt à appliquer des politiques pour un VPC, modifiez le connecteur GCP (voir Modifier un connecteur GCP, à la page 97) et activez la segmentation pour ce VPC.

Étiquettes d'inventaire de GKE, détails et état d'application

Pour afficher des informations sommaires sur un connecteur GCP, accédez à **Connector >** et choisissez GCP Connector (Connecteur GCP) dans la page Connectors (Connecteurs).

Pour afficher des informations sur l'inventaire, cliquez sur l'adresse IP d'une charge de travail particulière dans la page Scopes and Inventory (Portée et inventaire). Vous pouvez également accéder au profil d'inventaire à partir de l'onglet d'interface du profil VPC. Pour en savoir plus sur le profil d'inventaire, consultez *Profil d'inventaire*.

De même, pour afficher toutes les politiques concrètes sous le profil VPC, sous l'onglet Politiques concrètes du profil d'inventaire, accédez au profil VPC parent pour voir toutes les politiques concrètes sous le VPC.

Le profil VPC est accessible à partir de la page de configuration ou d'état d'application GCP (globale ou au sein d'un espace de travail). Vous pouvez afficher l'état de l'application et les politiques concrètes au niveau du VPC sur le profil VPC. Vous pouvez également afficher les politiques de pare-feu VPC combinées de toutes les interfaces dans l'onglet VPC Firewall Rules (politiques de pare-feu VPC).

Pour en savoir plus sur les étiquettes, consultez :

- *Étiquettes générées par les connecteurs infonuagiques*

- *Étiquettes liées aux grappes Kubernetes*

Résoudre les problèmes de connecteur GCP

Problème : La page Enforcement Status (État de la mise en application) indique qu'une politique concrète a été SKIPPED (IGNORÉE).

Solution : Ce problème se produit lorsque le nombre de règles dans la politique de pare-feu dépasse les limites GCP, telles que configurées dans le connecteur GCP.

Lorsqu'une politique concrète s'affiche comme SKIPPED (IGNORÉE), les nouveaux groupes de sécurité ne sont pas mis en œuvre et les groupes de sécurité existants sur GCP restent en vigueur.

Pour résoudre ce problème, voyez si vous pouvez consolider les politiques, par exemple en utilisant un sous-réseau plus grand dans une politique plutôt que plusieurs avec des sous-réseaux plus petits.

Contexte :

Des politiques concrètes sont générées pour chaque VPC lorsque la segmentation est activée. Ces politiques concrètes sont utilisées pour créer des politiques de pare-feu dans GCP. Cependant, GCP et Cisco Secure Workload comptabilisent les politiques différemment. Lors de la conversion de politiques Cisco Secure Workload en règles de pare-feu GCP dans les politiques de pare-feu, le mécanisme de comptage GCP est complexe. Pour plus de renseignements, voir GCP.

Problème : GCP autorise tout le trafic de manière inattendue

Solution : Vérifiez que la politique Catch-All (globale collectrice) dans Cisco Secure Workload est définie sur Deny (Refuser).

Services gérés Kubernetes s'exécutant sur GCP (GKE)

Vous pouvez utiliser un connecteur infonuagique pour recueillir des métadonnées à partir des grappes Google Kubernetes Engine (GKE) s'exécutant sur Google Cloud Platform (GCP).

Le connecteur rassemble toutes les métadonnées de nœuds, de services et d'espaces liées à toutes les grappes Kubernetes sélectionnées.

Exigences et prérequis

Exigences de Cisco Secure Workload : ce connecteur ne nécessite pas d'appliance virtuelle.

Exigences de la plateforme :

- Assurez-vous que vous disposez des autorisations dans GCP pour configurer l'accès requis pour ce connecteur.
- Chaque grappe GKE ne peut appartenir qu'à un seul connecteur GCP.
- Recueillez les informations décrites dans les tableaux de la section *Configurer un connecteur GCP*, ci-dessous.

Exigences GKE :

- Vous devez configurer les privilèges d'accès requis dans GKE.
- Pour prendre en charge les fonctionnalités des K8 gérés, les rôles requis par le compte de service sont les suivants :

- Le Compute Network Viewer (Visualiseur de réseau informatique) est un rôle IAM qui donne un accès en lecture seule à toutes les ressources réseau dans GCP.https://cloud.google.com/compute/docs/access/iam#compute.networkViewer
- Le Kubernetes Engine Viewer (Visualiseur de moteur Kubernetes) est un rôle de grappe GKE qui fournit un accès en lecture seule aux ressources des grappes GKE, telles que les nœuds, les pods et les objets d'API GKE. https://cloud.google.com/iam/docs/understanding-roles#kubernetes-engine-roles

Connecteurs d'identité

Le connecteur d'identités sert de pont entre Cisco Secure Workload et divers entrepôts d'identités, tels qu'OpenLDAP, Active Directory et Azure AD. Le connecteur vous permet de synchroniser les renseignements stockés dans les entrepôts d'identités sans intervention manuelle. Actuellement, vous pouvez configurer un connecteur d'identité pour acquérir les données des utilisateurs à partir de LDAP.

Configurer un connecteur OpenLDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole conçu pour récupérer des informations sur les utilisateurs, les groupes d'utilisateurs, les organisations et d'autres attributs. Son objectif principal est de stocker des données dans l'annuaire LDAP pour rationaliser la gestion des utilisateurs.

Note La version prise en charge pour l'acquisition de données OpenLDAP est OpenLDAP 2.6.

Configuration

Créez un connecteur d'identité pour LDAP dans Cisco Secure Workload afin d'établir la communication avec OpenLDAP.

Procédure

Étape 1 Dans le volet de navigation, choisissez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Connectors (Connecteurs)** .

Étape 2 Sélectionnez **Identity Connector** (Connecteur d'identité) et cliquez sur **Configure your new connector here** (Configurez votre nouveau connecteur ici).

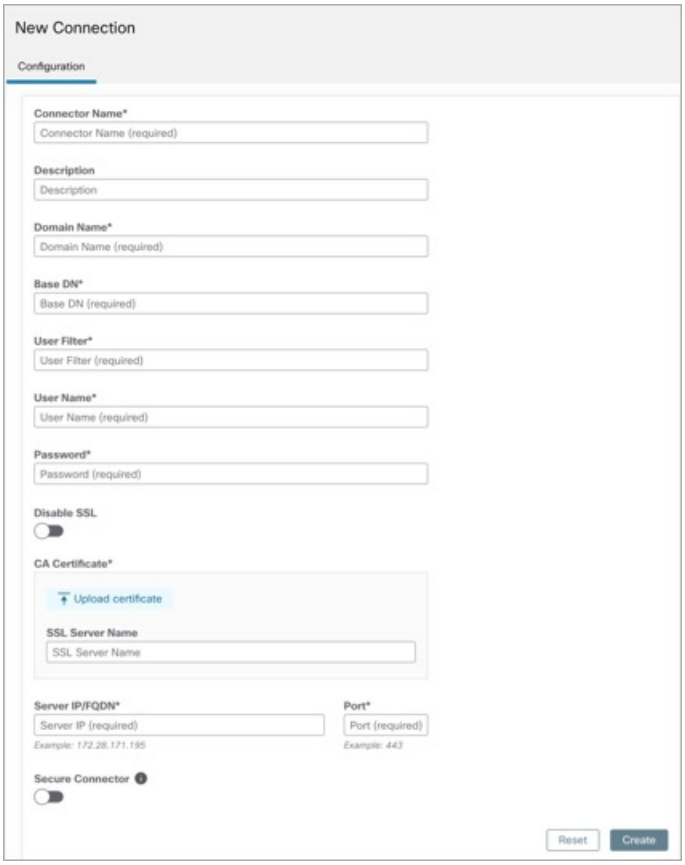
Étape 3 Sur la page **New Connection** (Nouvelle connexion), saisissez les détails comme suit :

Champs	Description
Nom du connecteur	Saisissez un nom pour le connecteur.
Description	Saisissez une description
Domain Name (Nom de domaine)	Saisissez un nom de domaine Le nom de domaine doit être unique dans la portée sélectionnée. Par exemple, csw.com.

Champs	Description
Nom unique de base	Saisissez le DN de base ou le nom distinctif qui sert de point de départ aux recherches dans l'arborescence. Par exemple, dc=csw, dc=com.
Filtre utilisateur	Saisissez un filtre pour définir des critères d'identification des entrées qui contiennent certains types de renseignements. Exemple 1 : pour identifier des utilisateurs, vous les distinguez en utilisant deux attributs objetClass, l'un défini sur « person » et l'autre sur « user ». Les critères de correspondance peuvent être `(&(objectClass=person)(objectClass=user))` Exemple 2 : pour récupérer toutes les entrées qui ont pour objet class=user et l'attribut « cn » contenant le mot « Marketing », le filtre de recherche peut être `(&(ObjectClass=user)(cn=*Marketing*))`
Nom d'utilisateur et **mot de passe**	Saisissez les renseignements d'authentification pour vous connecter au serveur OpenLDAP.
Certificat de l'autorité de certification	Chargez le certificat de l'autorité de certification et entrez le nom du serveur SSL utilisé par Cisco Secure Workload pour l'authentification. Sinon, **désactivez SSL**.
Server IP/FQDN and Port (Adresse IP du serveur/Nom de domaine complet et Port)	Saisissez l'adresse IP du serveur et le numéro de port.
Connecteur sécurisé	Activez si un connecteur sécurisé est utilisé pour canaliser les connexions de Cisco Secure Workload vers OpenLDAP. Avant d'activer cette option, vous devez avoir déployé un connecteur sécurisé. Pour en savoir plus, consultez la section Secure Connector (Connecteur sécurisé).

Étape 4 Cliquez sur **Create** (créer).

Illustration 45 : Configurer un nouveau connecteur



Un nouveau connecteur d'identité est créé et la communication entre Cisco Secure Workload et OpenLDAP est configurée.

Inventaire

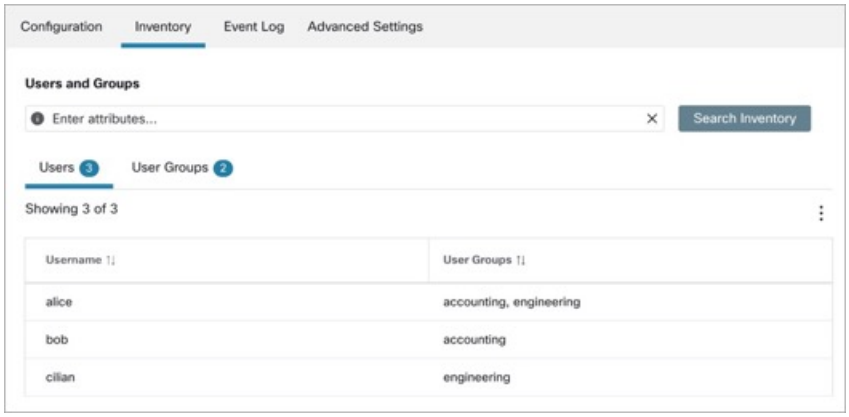
Lorsque la connexion entre Cisco Secure Workload et OpenLDAP est établie, vous pouvez afficher une liste des **utilisateurs** et **des groupes d'utilisateurs** sous l'onglet **Inventory** (inventaire). Tous les groupes d'utilisateurs auxquels un utilisateur appartient sont affichés sous l'onglet **Users** (utilisateurs). Seuls les groupes d'utilisateurs uniques sont affichés dans l'onglet User Groups (groupes d'utilisateurs).

Procédure

Étape 1 Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'information pour afficher les propriétés à filtrer.

Étape 2 Cliquez sur l'icône de menu pour télécharger les données au format JSON ou CSV.

Illustration 46 : Utilisateurs et groupes d'utilisateurs



Remarque La limite recommandée pour le nombre d'utilisateurs affichés est de 300 000, tandis que pour les groupes d'utilisateurs, elle est de 30 000.

Journal des événements

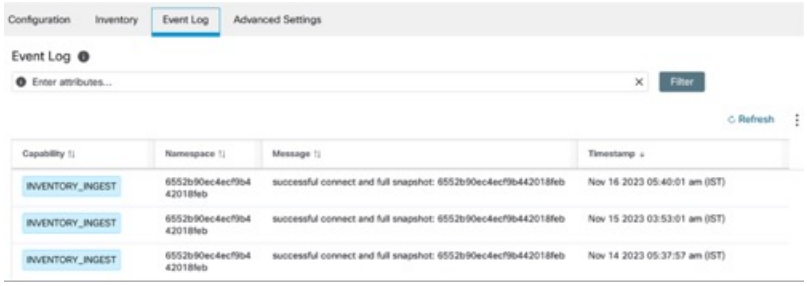
L'onglet Event Log (journal des événements) affiche des informations, des avertissements et des erreurs qui se produisent lors de l'établissement de la connexion avec OpenLDAP.

Procédure

Étape 1 Saisissez les attributs à filtrer. Passez le curseur sur l'icône d'information pour afficher les propriétés à filtrer.

Étape 2 Cliquez sur l'icône de menu pour télécharger les données au format JSON ou CSV.

Illustration 47 : Journal des événements



Remarque Les codes de couleur des journaux sont les suivants : information (bleu), avertissement (ambre) et erreur (red).

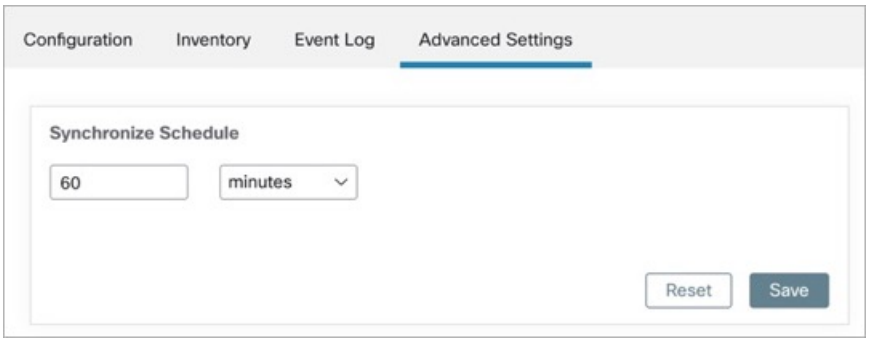
Paramètres avancés

Procédure

Étape 1 Sous **Synchronize Schedule** (Synchroniser la planification), vous pouvez choisir une fréquence à laquelle Cisco Secure Workload synchronise les données d'utilisateur à partir du serveur LDAP.

Étape 2 Dans le champ **User Attributes** (attributs de l'utilisateur), saisissez jusqu'à six attributs utilisateur à afficher.

Illustration 48 : Paramètres avancés



Alertes du connecteur

Un appareil ou un service crée une alerte de connecteur lorsqu'il présente un comportement anormal.

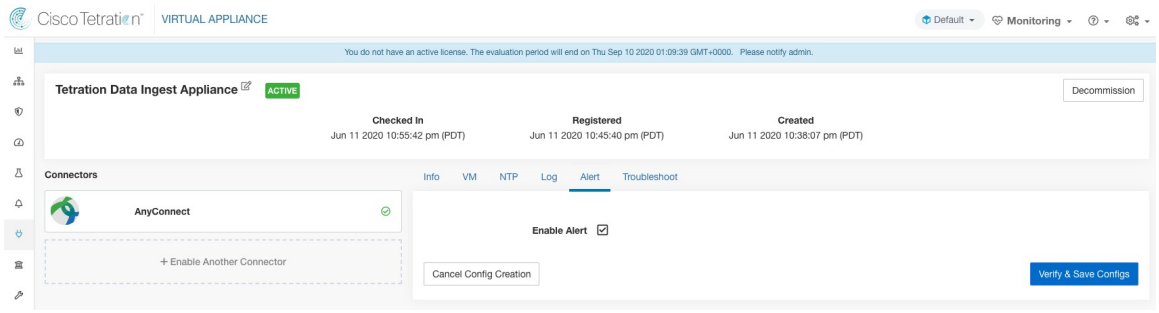
Configuration des alertes

La configuration des alertes pour les appareils et les connecteurs vous permet de générer des alertes pour divers événements. Dans la version 3.4, cette configuration active tous les types d'alertes potentiellement possibles pour l'appareil/connecteur configuré.

Nom du paramètre	Type	Description
Enable Alert	case	L'alerte doit-elle être activée?

Note La valeur par défaut pour *Enable Alert* est *vrai*.

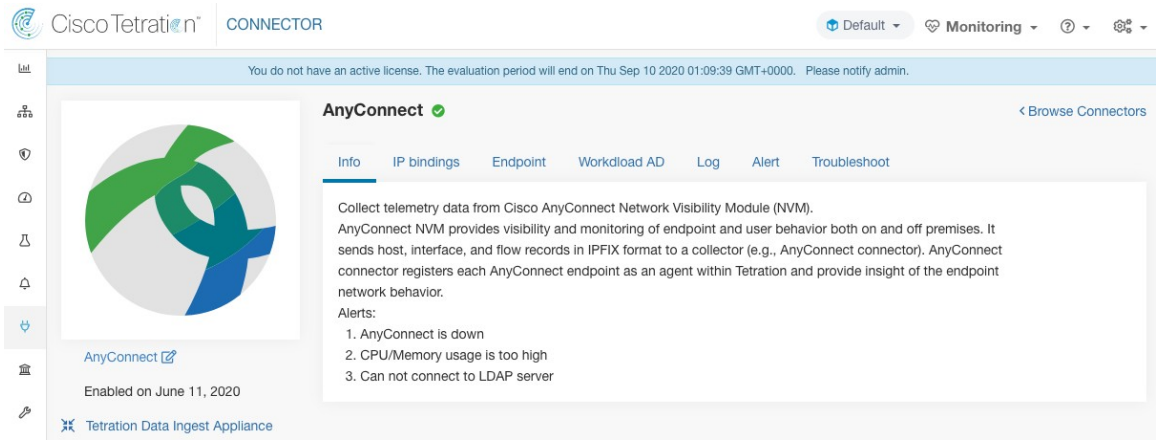
Figure 49: Afficher la configuration des alertes sur un appareil d'acquisition de données Cisco Secure Workload



Type d'alerte

L'onglet Info des pages de l'appareil et du connecteur contient différents types d'alertes spécifiques à chaque appareil et connecteur.

Figure 50: Informations sur la liste d'alertes



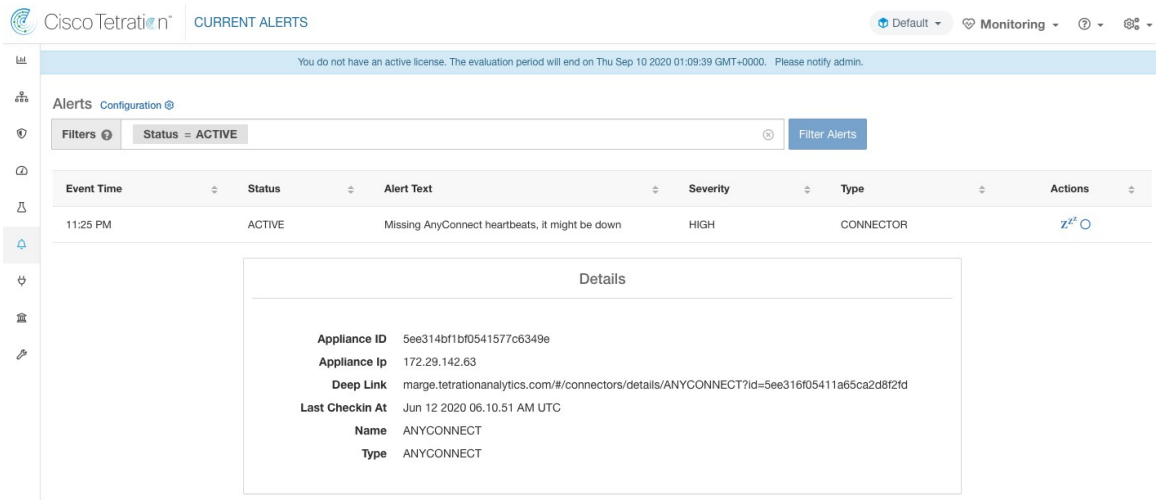
Appareil/connecteur en panne

Une alerte est générée lorsqu'un appareil (ou un connecteur) est potentiellement en panne en raison de pulsations manquantes de l'appareil ou du connecteur.

Texte d'alerte : Missing <Appliance/Connector> heartbeats, it might be down (signaux d'activité manquants <Appliance/Connector>, il est peut-être en panne).

Gravité : élevée

Figure 51: Alerte de connecteur en panne



appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : tous

Utilisation du système des appareils et des connecteurs

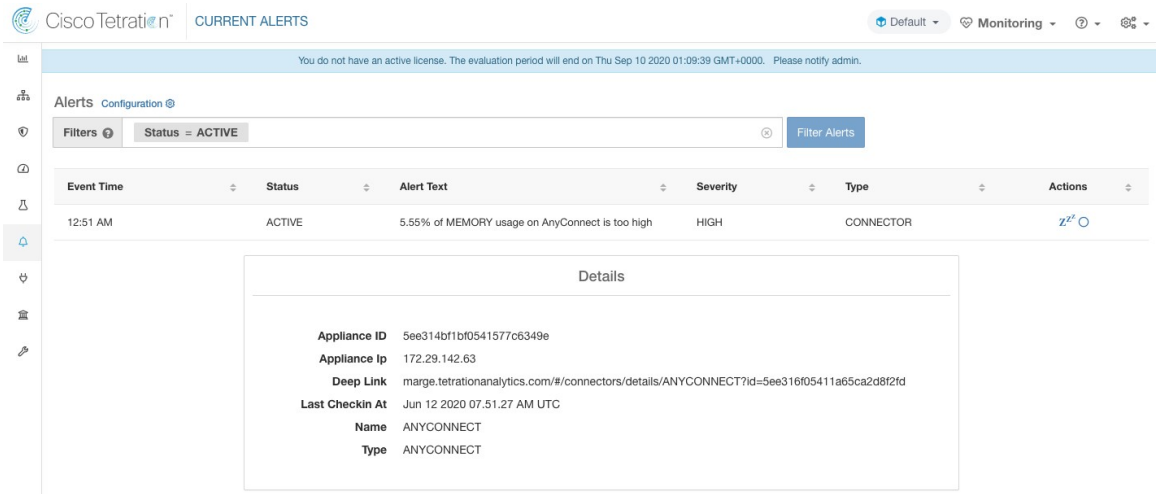
Lorsque l'utilisation du système (CPU, mémoire et disque) est supérieure à 90 % sur un appareil (et un connecteur). L'appareil (et/ou le connecteur) génère une alerte informationnelle pour indiquer qu'il gère actuellement une charge système accrue.

Il est normal que les appareils et les connecteurs consomment plus de 90 % des ressources système lors d'une activité de traitement intensive.

Texte de l'alerte :<Number> d'utilisation du processeur, de la mémoire/du disque sur <Appliance/Connector> est trop élevé.

Gravité : élevée

Figure 52: Alerte d'utilisation du système du connecteur trop élevée



appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : tous

Erreur de configuration du connecteur

Lorsque vous essayez de connecter un connecteur configuré à un serveur configuré et que la configuration échoue, le système génère une alerte pour indiquer un problème potentiel de configuration après son acceptation et son déploiement.

Par exemple, le connecteur AnyConnect peut accepter une configuration LDAP, valider et accepter la configuration. Cependant, pendant le fonctionnement normal, il est possible que la configuration ne soit plus valide.

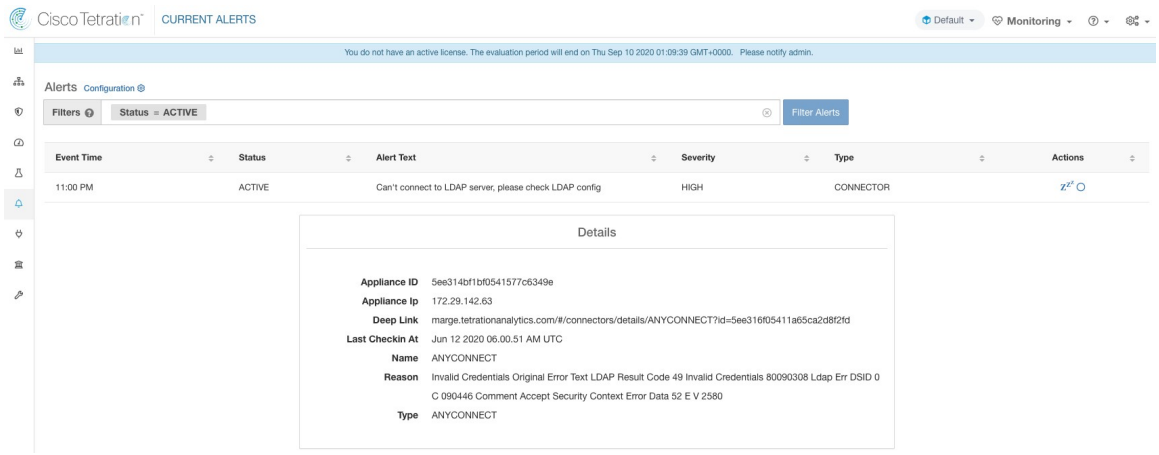
Une alerte capture le scénario et indique que vous devez prendre des mesures correctives pour mettre à jour la configuration.

Texte d'alerte : Impossible de se connecter au serveur <Appareil/Connecteur>, vérifier la configuration de <Appareil/Connecteur>.

Gravité : élevée, faible

Serveur	Connecteur
Serveur LDAP	AnyConnect, F5, ISE, WDC
Serveur ISE	ISE
Serveur ServiceNow	ServiceNow

Figure 53: Alerte pour erreur d'état de configuration

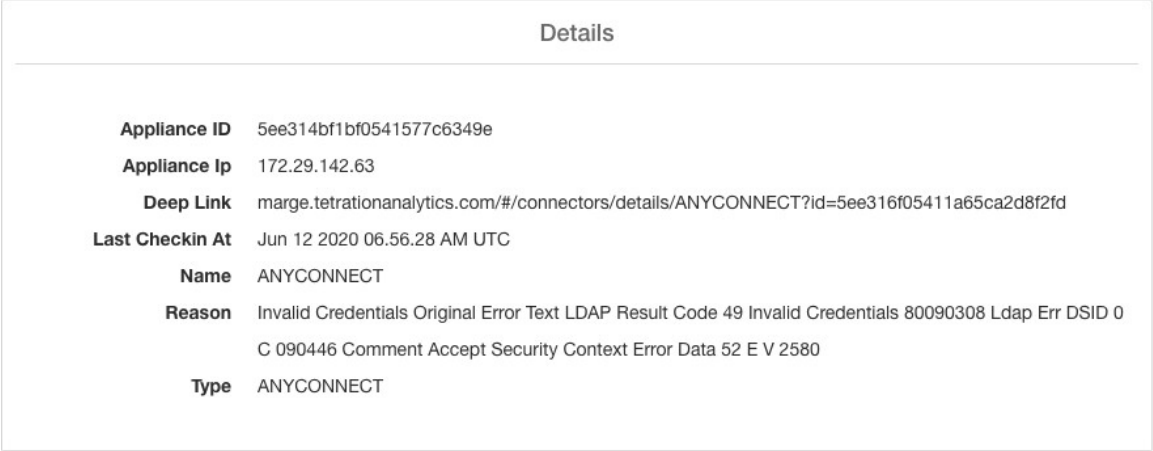


appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : AnyConnect, F5, ISE, WDC et ServiceNow.

Détails de l'alerte de l'interface utilisateur du connecteur

Figure 54: Détails de l'alerte de l'interface utilisateur du connecteur



Détails de l'alerte

Consultez Common Alert Structure (Structure d'alerte commune) pour obtenir la structure générale des alertes et des informations sur les champs. La structure des champs *alert_details* contient les sous-champs suivants pour les alertes de connecteur.

Champ	Type	Description
ID de dispositif	Chaîne	ID de dispositif
IP d'appareil	Chaîne	IP d'appareil
ID du connecteur	Chaîne	ID du connecteur
Adresse IP du connecteur	Chaîne	Adresse IP du connecteur
Lien profond	Lien hypertexte	Redirection vers la page de l'appareil/du connecteur
Last CheckIn At	Chaîne	Heure de la dernière connexion
Nom	Chaîne	Nom de l'appareil/du connecteur
Motif	Chaîne	Raison pour laquelle l'appareil ou le connecteur ne peut pas se connecter à Cisco Secure Workload
Type	Chaîne	Type d'appareil/de connecteur

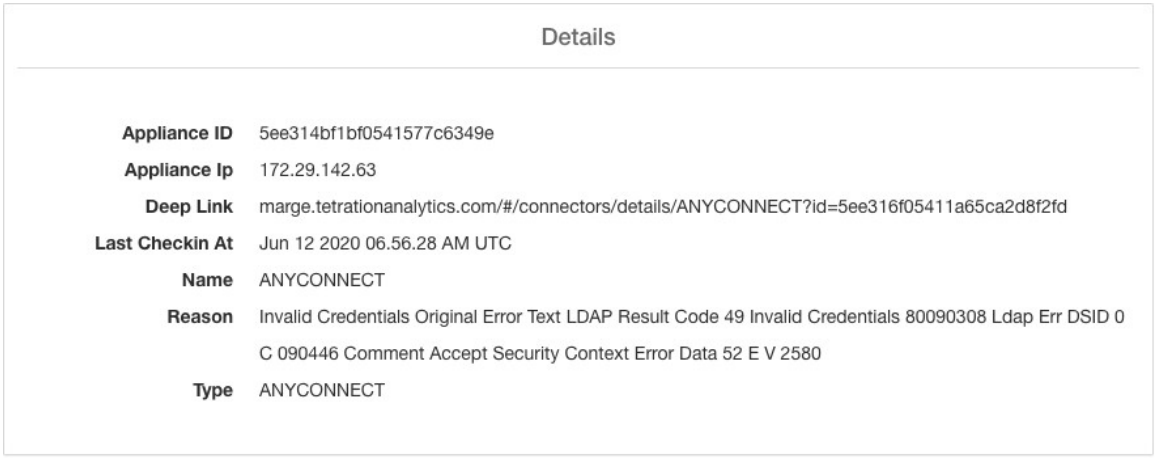
Exemple de détails d'alerte

Après avoir analysé alert_details comme JSON (n'est pas une chaîne), il s'affichera comme suit.

```
    {
      "Appliance ID": "5f1f3d26d674b01832c6792a",
      "Connector ID": "5f1f3e47baba512a70abee43",
      "Connector IP": "172.29.142.22",
      "Deep Link":
"bingo.tetrationanalytics.com/#/connectors/details/F5?id=5f1f3e47baba512a70abee43",
      "Last checkin at": "Aug 04 2020 20.37.33 PM UTC",
      "Name": "F5",
      "Reason": "Invalid Credentials (Original error text: LDAP Result Code 49 \"Invalid
Credentials\": )",
      "Type": "F5"
    }
```


Détails de l'alerte de l'interface utilisateur du connecteur

Figure 55: Détails de l'alerte de l'interface utilisateur du connecteur



Gestion du cycle de vie des connecteurs

Les connecteurs peuvent être activés, déployés, configurés, dépannés et supprimés directement à partir de Cisco Secure Workload.

Activation d'un connecteur

Sur la page Connecteurs (**Manage (Gestion)** > **Connectors (Connecteurs)**), vous pouvez sélectionner et activer un connecteur. Le connecteur peut être déployé sur une nouvelle appliance virtuelle (qui doit d'abord être mise en service et devenir *active* avant qu'un connecteur ne puisse être activé sur celle-ci) ou sur une appliance virtuelle existante. Une fois l'appliance virtuelle choisie, Cisco Secure Workload envoie le paquet RPM du connecteur à l'appliance.

Lorsque le contrôleur d'appareil sur l'appliance choisie reçoit le RPM, il effectue ce qui suit :

1. Créer une image Docker à l'aide du paquet RPM reçu de Cisco Secure Workload. Cette image Docker inclut la configuration nécessaire pour communiquer avec le sujet Kafka sur lequel les messages de gestion de l'appliance sont envoyés. Cela permet au service instancié à partir de cette image de pouvoir envoyer et recevoir des messages pour la gestion du connecteur correspondant.

2. Créer un conteneur Docker à partir de l'image Docker.
3. Sur l'appareil d'acquisition Cisco Secure Workload, les tâches supplémentaires suivantes sont effectuées.
   - Un logement (slot) libre est identifié et l'adresse IP correspondante est déterminée.
   - Les ports d'écoute des connecteurs (par exemple, les ports 4729 et 4739 sur le connecteur NetFlow pour recevoir les enregistrements de flux de commutateurs et de routeurs compatibles avec NetFlow V9 ou IPFIX) sont accessibles à l'hôte à l'adresse IP correspondant au logement choisi.
   - Un volume Docker est créé et ajouté au conteneur.
4. Le conteneur Docker est démarré et il exécute le connecteur en tant que service géré *surveillé*. Le service démarre *le contrôleur de services* en tant que *tet-controller,* qui s'enregistre auprès de Cisco Secure Workload et génère le service de connecteur proprement dit.

Figure 56: Images de Docker

```
[root@beretta-ingest-1 tetter]# docker images
REPOSITORY                                                TAG                 IMAGE ID            CREATED             SIZE
netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow    5d379fac6e37d85f2bdeff45   2635145b44c8        About a minute ago   650MB
tet-service-base                                          latest              6be171bbe648        4 days ago          519MB
artifacts.tet.wtf:6555/centos                             7.3.1611            c5d48e81b986        4 months ago        192MB
[root@beretta-ingest-1 tetter]#
```

Figure 57: Volumes de Docker

```
[root@beretta-ingest-1 tetter]# docker volume ls
DRIVER              VOLUME NAME
local               373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439
[root@beretta-ingest-1 tetter]#
```

Figure 58: Conteneurs Docker

```
[root@beretta-ingest-1 tetter]# docker ps
CONTAINER ID        IMAGE                                                                                    COMMAND                  CREATE
D              STATUS              PORTS                                                                NAMES
2c7a7ed4f853        netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45   "/usr/bin/supervisor…"   About
a minute ago   Up About a minute   172.29.142.26:4729->4729/udp, 172.29.142.26:4739->4739/udp   nf-5d379fac6e37d85f2bdeff45
[root@beretta-ingest-1 tetter]#
```

Figure 59: Logement utilisé par le conteneur Docker et liste des ports accessibles


```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


Figure 60: Liste des ports rendus accessibles par le conteneur Docker


```
[root@beretta-ingest-1 tetter]# docker port 2c7a7ed4f853
4729/udp -> 172.29.142.26:4729
4739/udp -> 172.29.142.26:4739
[root@beretta-ingest-1 tetter]#
```


Figure 61: Volume Docker monté sur un conteneur


```
[root@beretta-ingest-1 tetter]# docker inspect --format='{{json .Mounts}}' 2c7a7ed4f853
[{"Type":"volume","Name":"373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439","Source":"/var/lib/docker/volumes/373b5b6
82a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439/_data","Destination":"/local/tetration","Driver":"local","Mode":"z","RW":tr
ue,"Propagation":""}]
[root@beretta-ingest-1 tetter]#
```


Le contrôleur de services est responsable des fonctions suivantes :

1. **Registration**(enregistrement) : enregistre le connecteur auprès de Cisco Secure Workload. Tant que le connecteur n'est pas enregistré et marqué *Enabled* (activé), aucune mise à jour de configuration ne peut

être envoyée au connecteur. Lorsque Cisco Secure Workload reçoit une demande d'enregistrement pour un connecteur, il met à jour l'état du connecteur à *Enabled* (activé).

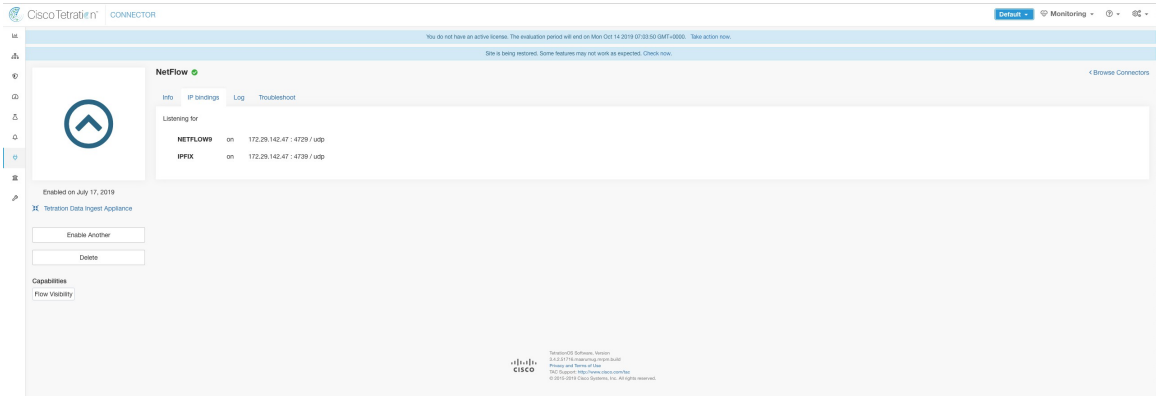
2. **Mises à jour de la configuration sur le connecteur** : teste et applique les mises à jour de configuration sur le connecteur. Pour en savoir plus, consultez Gestion de la configuration sur les connecteurs et les appliances virtuelles.
3. **Commandes de dépannage sur le connecteur** : exécute les commandes autorisées sur le service de connecteur pour le dépannage et le débogage des problèmes sur le service de connecteur. Consultez la section Dépannage (Dépannage) pour en savoir plus.
4. **Heartbeats** (pulsations) : envoie régulièrement des pulsations et des statistiques à Cisco Secure Workload pour signaler l'intégrité du connecteur. Pour en savoir plus, consultez Surveillance d'une appliance virtuelle.

Affichage des informations relatives au connecteur

Connecteurs activés : Vous pouvez obtenir une liste de tous les connecteurs activés en cliquant sur **Manage (Gestion)** > **Connectors (Connecteurs)** dans la barre de navigation à gauche de la fenêtre.

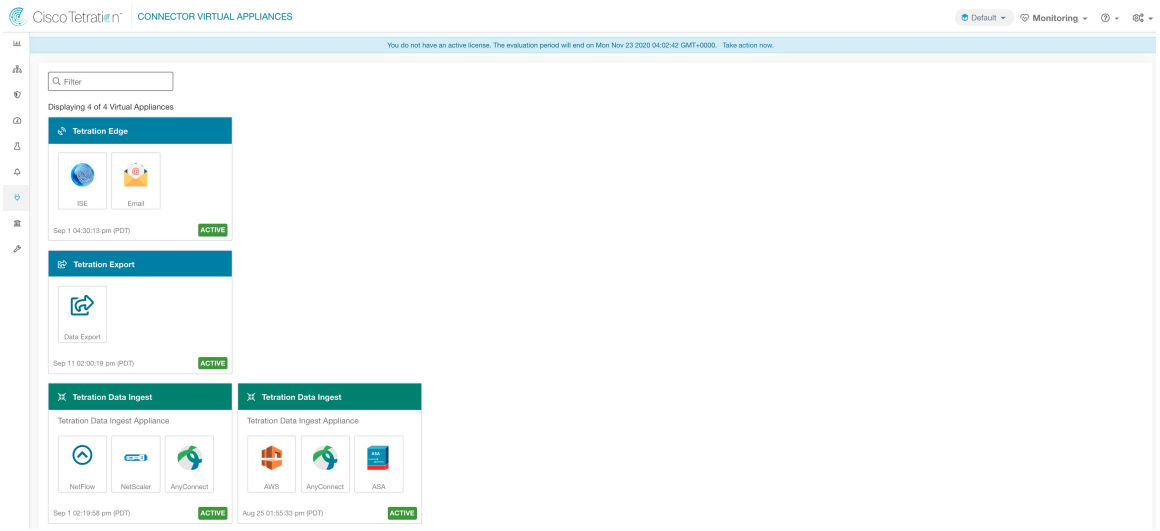
Détails du connecteur : Vous pouvez obtenir des détails sur le connecteur en cliquant sur le connecteur. Cette page affiche les liaisons de port (le cas échéant) qui peuvent être utilisées pour configurer les éléments de réseau en amont afin d'envoyer des données de télémétrie à l'adresse IP et au port appropriés.

Figure 62: Détails du connecteur



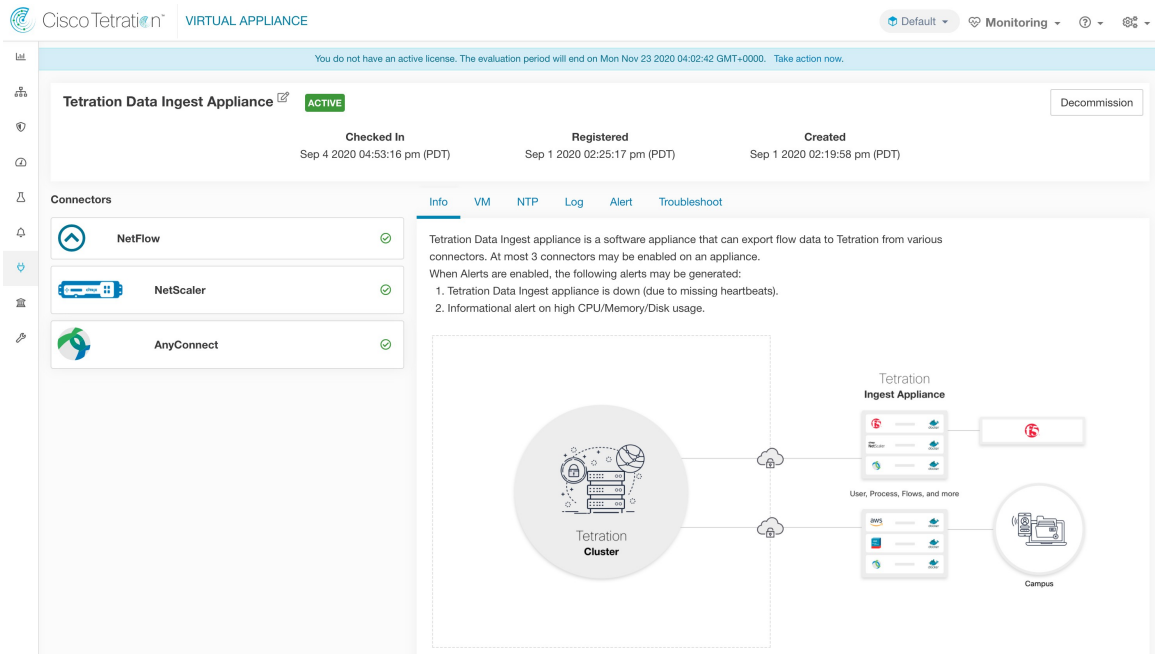
Appliances virtuelles déployées : Vous trouverez une liste des appliances virtuelles déployées à l'adresse suivante : **Manage (Gestion)** > **Virtual Appliances (Appliances virtuelles)** .

Figure 63: Liste des appliances virtuelles déployées



Détails de l'appliance virtuelle Pour obtenir une vue détaillée d'une appliance, cliquez sur celle-ci directement dans la *Liste des appliances virtuelles déployées*.

Figure 64: Détails sur l'appliance et les connecteurs



Suppression d'un connecteur

Lorsqu'un connecteur est supprimé, le contrôleur d'appareil sur l'appareil où le connecteur est activé reçoit un message lui demandant de supprimer les services créés pour le connecteur. Le contrôleur de l'appareil effectue les tâches suivantes :

1. Arrêter le conteneur Docker correspondant au connecteur.
2. Supprimer le conteneur Docker.
3. Si le connecteur est déployé sur un appareil d'acquisition Cisco Secure Workload et qu'il expose des ports, retirer le volume Docker qui a été monté sur le conteneur.
4. Supprimer l'image Docker qui a été créée pour le connecteur.
5. Enfin, renvoyer un message à Cisco Secure Workload pour indiquer l'état de la demande de suppression.

Surveillance d'un connecteur

Les services du connecteur envoient régulièrement des signaux de présence et des statistiques à Cisco Secure Workload. L'intervalle du signal de présence (heartbeat) est de 5 minutes. Les messages heartbeat comprennent des statistiques sur l'intégrité du service, notamment des statistiques du système, des statistiques de processus et des statistiques sur le nombre de messages envoyés, reçus ou erronés sur le sujet Kafka utilisé pour la gestion de l'appareil. En outre, ils comprennent les statistiques exportées par le service de connecteur lui-même.

Toutes les métriques sont disponibles dans *Digger* (OpenTSDB) et sont annotées avec l'ID de l'appareil, l'ID du connecteur et le nom de la portée racine. En outre, les tableaux de bord Grafana pour les services du connecteur sont également disponibles pour les mesures importantes du service.

Appliances virtuelles pour les connecteurs

La plupart des connecteurs sont déployés sur des appliances virtuelles Cisco Secure Workload. Vous déploierez les appareils virtuels requis sur un hôte ESXi dans VMware vCenter en utilisant les modèles OVA ou sur d'autres hyperviseurs basés sur KVM à l'aide de l'image QROW2. La procédure de déploiement d'appliances virtuelles est décrite dans la section Deploying a Virtual Appliance.

Types d'appliances virtuelles

Chaque connecteur nécessitant une appliance virtuelle peut être déployé sur l'un des deux types d'appliances virtuelles.

Acquisition de Cisco Secure Workload

L'appareil d'acquisition Cisco Secure Workload est une appliance logicielle qui peut exporter des observations de flux vers Cisco Secure Workload à partir de divers connecteurs.

Fiche technique

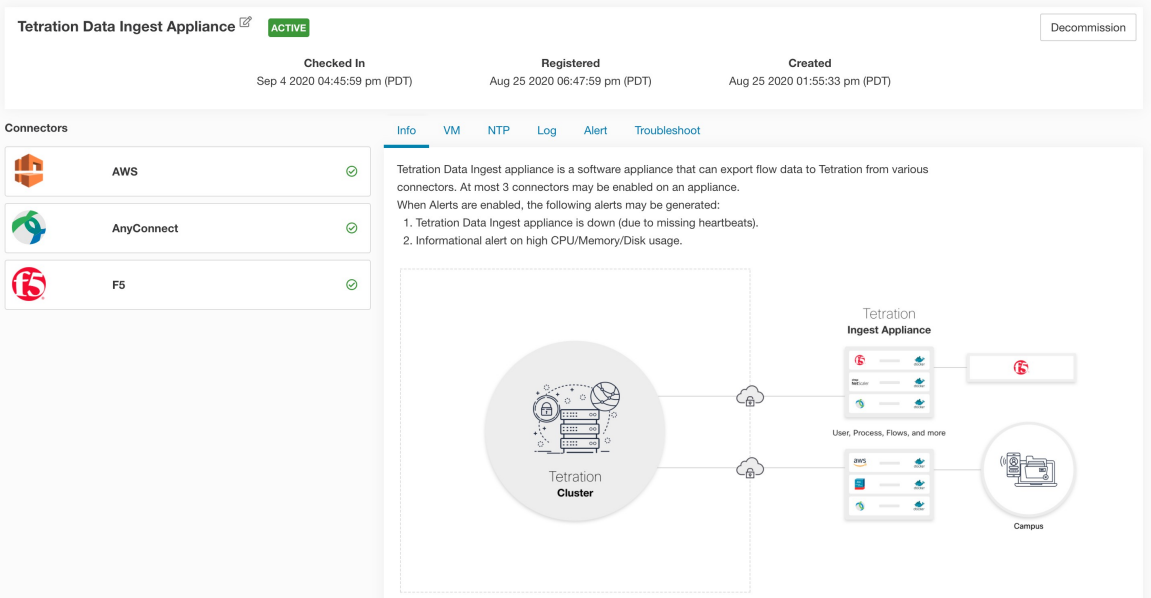
- Nombre de cœurs de processeur : 8
- Mémoire : 8 Go
- Stockage : 250 Go
- Nombre d'interfaces réseau : 3
- Nombre de connecteurs sur un appareil : 3

- Système d'exploitation : CentOS 7.9 (Cisco Secure Workload 3.8.1.19 et versions ultérieures), AlmaLinux 9.2 (Cisco Secure Workload 3.8.1.36 ou versions ultérieures)

Consultez les limites importantes à l'adresse Appliances virtuelles de charge de travail sécurisée pour les connecteurs.

Note Chaque portée racine sur Cisco Secure Workload ne peut avoir qu'un maximum de 100 dispositifs d'acquisition Cisco Secure Workload déployés.

Figure 65: Dispositif d'acquisition Cisco Secure Workload



L'appareil d'acquisition Cisco Secure Workload permet à un maximum de trois connecteurs d'être activés sur un dispositif. Plusieurs instances d'un même connecteur peuvent être activées sur le même appareil. Pour l'appareil d'acquisition ERSPAN, trois connecteurs ERSPAN sont toujours mis en service automatiquement. Un grand nombre des connecteurs déployés sur l'appareil d'acquisition collecte la télémétrie de divers points du réseau. Ces connecteurs doivent être à l'écoute sur des ports spécifiques de l'appareil. Chaque connecteur est par conséquent lié à l'adresse IP et au port par défaut sur lequel le connecteur doit être à l'écoute pour collecter des données de télémétrie. Par conséquent, chaque adresse IP est essentiellement un emplacement qu'un connecteur occupe sur l'appareil. Lorsqu'un connecteur est activé, un emplacement est occupé (et donc l'adresse IP correspondant à l'emplacement). De plus, lorsqu'un connecteur est désactivé, l'emplacement occupé par le connecteur est libéré (et donc l'adresse IP correspondant à l'emplacement). Reportez-vous à la section relatives à *l'acquisition de Cisco Secure Workload* pour savoir comment l'appareil d'acquisition assure la maintenance de l'état des emplacements.

Figure 66: Emplacements de l'appareil d'acquisition Cisco Secure Workload

```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


Configurations autorisées

- *NTP* : configurez le NTP sur l'appareil. Pour en savoir plus, consultez Configuration du protocole NTP.
- *Log (Journal)* : Configurez la journalisation sur l'appareil. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Cisco Secure Workload Edge

Cisco Secure Workload Edge est un appareil de contrôle qui transmet des alertes à divers notifications et recueille les métadonnées d'inventaire provenant de contrôleurs d'accès réseau comme Cisco ISE. Dans un appareil de périphérie Cisco Secure Workload, tous les connecteurs de notification d'alerte (comme Syslog, Courriel, Slack, PagerDuty et Kinesis), le connecteur ServiceNow, le connecteur de charge de travail AD et le connecteur ISE, peuvent être déployés.

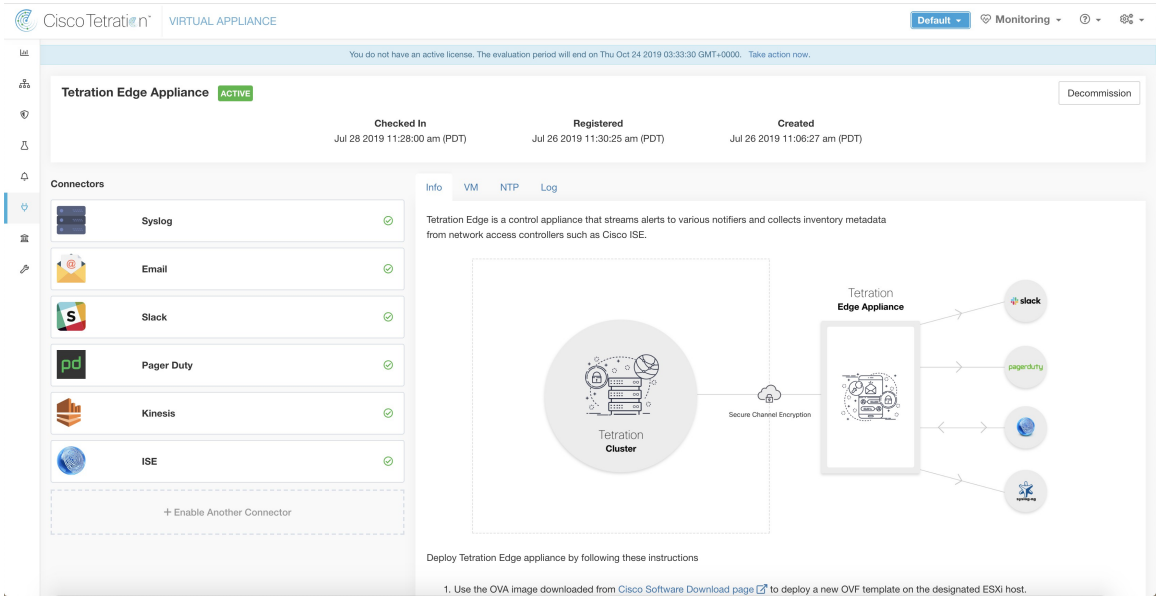
Fiche technique

- Nombre de cœurs de processeur : 8
- Mémoire : 8 Go
- Stockage : 250 Go
- Nombre d'interfaces réseau : 1
- Nombre de connecteurs sur un appareil : 8
- Système d'exploitation : CentOS 7.9 (Cisco Secure Workload 3.8.1.19 et versions ultérieures), AlmaLinux 9.2 (Cisco Secure Workload 3.8.1.36 ou versions ultérieures)

Consultez les limites importantes à l'adresse Appliances virtuelles de charge de travail sécurisée pour les connecteurs.

Note Chaque portée racine sur Cisco Secure Workload ne peut avoir qu'un seul appareil de périphérie Cisco Secure Workload déployé.

Figure 67: Appareil de périphérie Cisco Secure Workload



Les connecteurs déployés sur l'appareil de périphérie Cisco Secure Workload n'écoutent pas sur les ports. Par conséquent, les conteneurs Docker instanciés pour les connecteurs sur l'appareil de périphérie Cisco Secure Workload n'exposent aucun port à l'hôte.

Configurations autorisées

- *NTP* : configurez le NTP sur l'appareil. Pour en savoir plus, consultez Configuration du protocole NTP.
- *Log (Journal)* : Configurez la journalisation sur l'appareil. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Deploying a Virtual Appliance

You will deploy virtual appliances on an ESXi host in VMware vCenter or other KVM-based hypervisors such as Red Hat Virtualization. This procedure will prompt you to download virtual appliance OVA template or QCOW2 image from the Cisco Software Download page.

Attention To deploy a Cisco Secure Workload external appliance, the ESXi host where the appliance is created should have the following specifications:

- **vSphere**: version 5.5 or better.
- **CPU**: at least 2.2 GHz per core, and has enough reservable capacity for the appliance.
- **Memory**: at least enough space to fit the appliance.

To deploy a virtual appliance to collect data from connectors:

Procedure

Étape 1 In the Cisco Secure Workload web portal, choose **Manage** > **Virtual Appliances** from the navigation bar on the left.

Étape 2 Click **Enable a Connector**. The type of virtual appliance you need to deploy depends on the type of connector you are enabling.

Étape 3 Click the type of connector for which you need to create the virtual appliance. For example, click the NetFlow connector.

Étape 4 On the connector page, click **Enable**.

Étape 5 If you see a notice telling you that you need to deploy a virtual appliance, click **Yes**. If you do not see this notice, you may already have a virtual appliance that this connector can use, in which case you do not need to perform this procedure.

Étape 6 Click the link to download the OVA template or QCOW2 image for the virtual appliance. Leave the wizard open on your screen without clicking anything else.

Étape 7 Use the downloaded:

- OVA to deploy a new OVF template on a designated ESXi host.
  - Please follow Deploy an OVF Template for instructions on how to deploy an OVA on a vSphere Web Client.
  - Ensure that the deployed VM settings match the recommended configuration for the virtual appliance type.
  - **Do not power on the deployed VM**
- QCOW2 image to create a new VM on KVM hypervisors such as Red Hat Virtualization.

Étape 8 After the VM is deployed, but before you power it on, return to the virtual appliance deployment wizard in the Cisco Secure Workload web portal.

Étape 9 Click **Next** in the virtual appliance deployment wizard.

Étape 10 Configure the virtual appliance by providing IP address(es), gateway(s), hostname, DNS, proxy server settings and docker bridge subnet configuration. Please refer to the screenshot for *Configuring the VM with network parameters*.

Note For NetFlow, ERSPAN, and ISE connectors, IPv6 addresses (dual stack mode) can be provided. However, do note that dual stack support is a BETA feature. For more information on the requirements and limitations for dual-stack mode, see the Cisco Cisco Secure Workload Upgrade Guide

- If the appliance needs to use proxy server to reach Secure Workload, please check the box *Use proxy server to connect to Secure Workload*. If this is not set correctly, connectors may not be able to communicate with Cisco Secure Workload for control messages, register connectors, and send flow data to Cisco Secure Workload collector.
- If the IP address(es) and gateways(s) of the appliance conflict with the default docker bridge subnet (*172.17.0.1/16*), the appliance can be configured with a customized docker bridge subnet specified in *Docker Bridge (CIDR format)* field. This requires appliance OVA 3.3.2.16 or later.

Étape 11 Click **Next**.

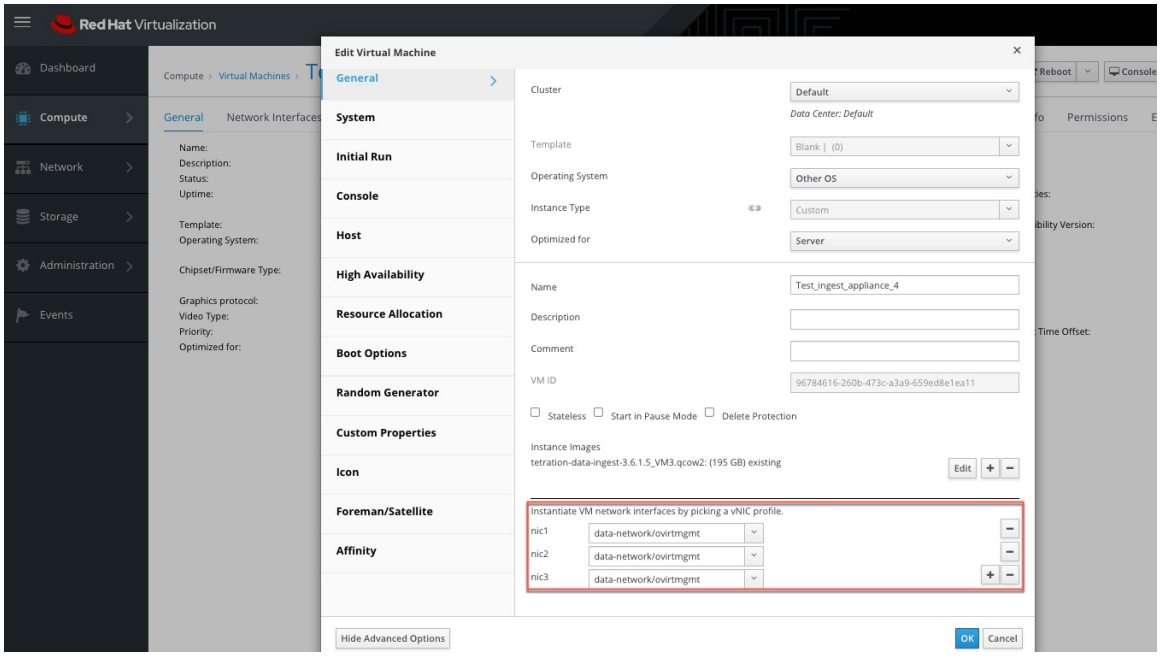
Étape 12 In the next step, a VM configuration bundle will be generated and available for download. Download the VM configuration bundle. Please refer to the screenshot for *Download the VM configuration bundle*.

Étape 13 Upload the VM configuration bundle to the datastore corresponding to the target ESXi host or other virtualization host.

Étape 14 [**Applicable only when using QCOW2 image**] Complete the following configurations on the other virutalization host where you have uploaded the VM configuration bundle:

- For ingest appliances, configure three network interfaces.

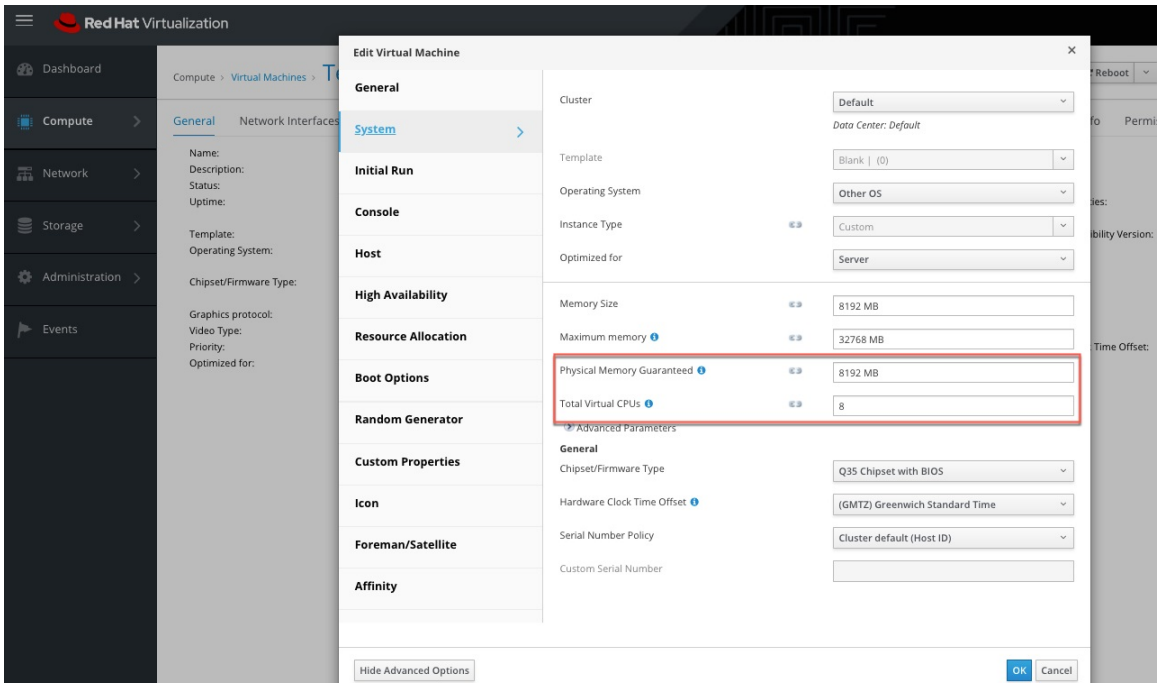
Figure 68: Example of configuring network interfaces in KVM-based environments



- In the memory allocation, specify the minimum requirement of 8192 MB of RAM.

- Specify the total number of virtual CPUs to be 8.

Figure 69: Example of configuring system resources in KVM-based environments



Étape 15 Edit the VM settings and mount the VM configuration bundle from the datastore to the CD/DVD drive. Please make sure to select **Connect at Power On** checkbox.

Étape 16 Power on the deployed VM.

Étape 17 Once the VM boots up and configures itself, it will connect back to Secure Workload. This may take a few minutes. The appliance status on Cisco Secure Workload should transition from *Pending Registration* to *Active*. Please refer to the screenshot for *Secure Workload Ingest appliance in Pending Registration state*.

Note We do not recommend vMotion to be enabled for Cisco Secure Workload external appliances.

Note We recommend to use Cisco Secure Workload external appliance OVAs as-is and to reserve 8 vCPU cores and 8192 MB of memory for QCOW2 images to deploy VMs. If sufficient resources are not available, the VM setup script would fail after the boot.

Once the appliance is *Active*, connectors can be enabled and deployed on it.

Figure 70: ploying a Cisco Secure Workload Ingest appliance

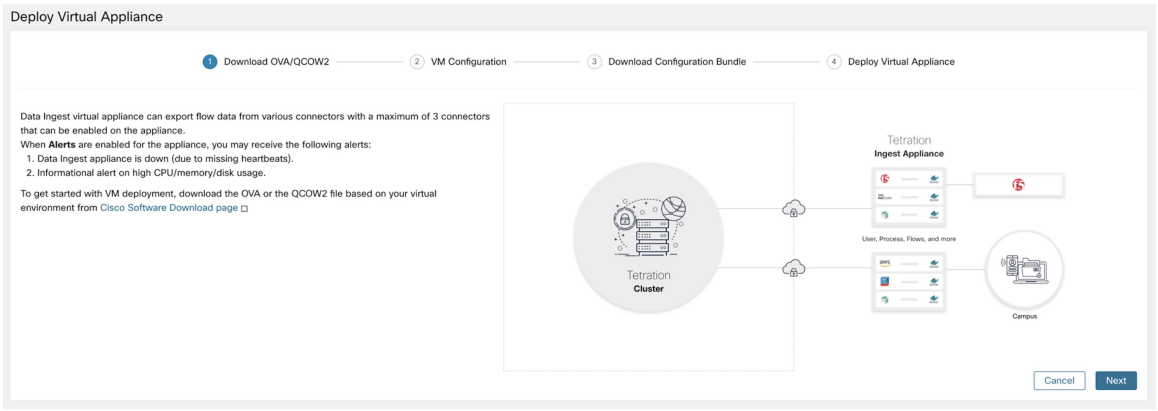


Figure 71: Configuring the VM with network parameters

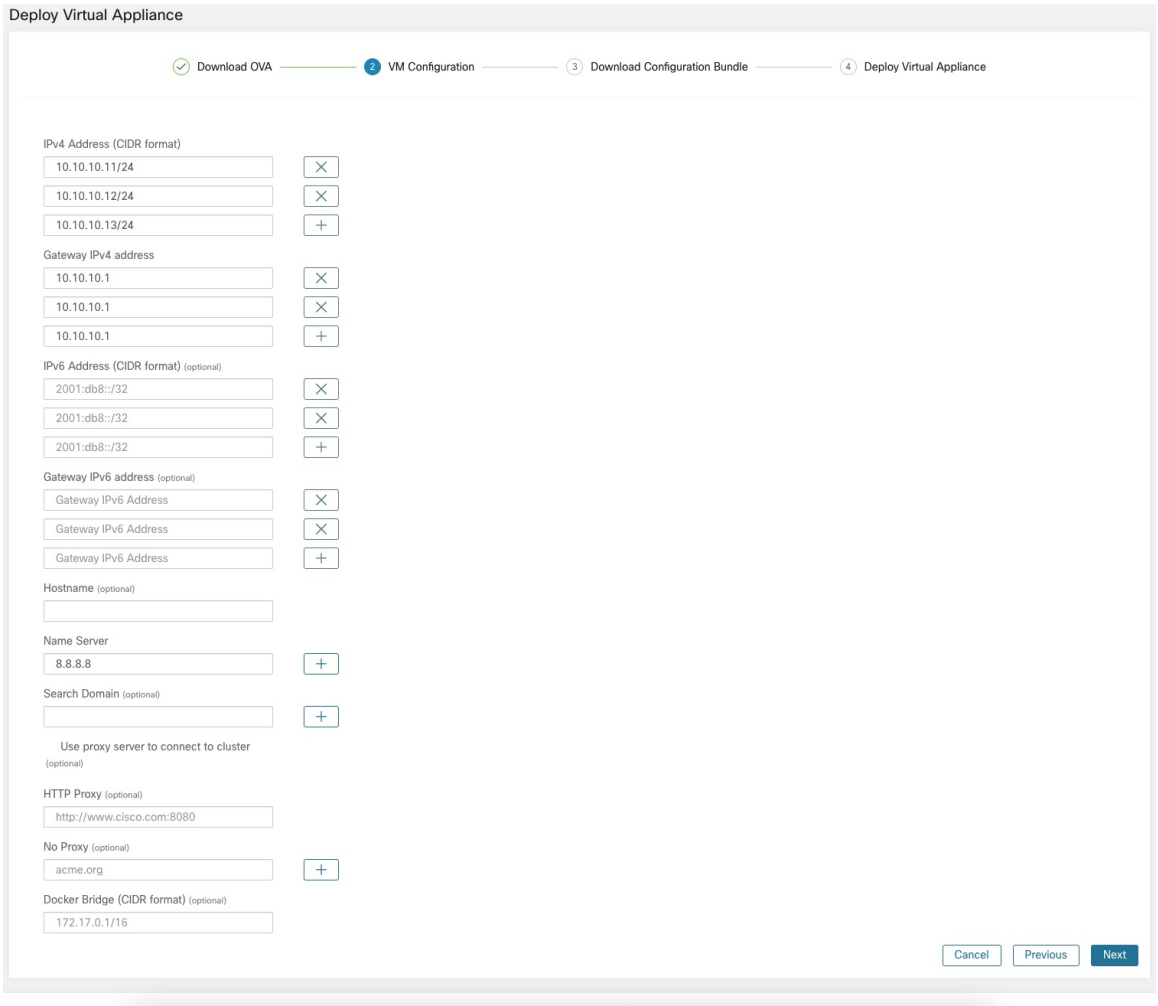


Figure 72: Download the VM configuration bundle

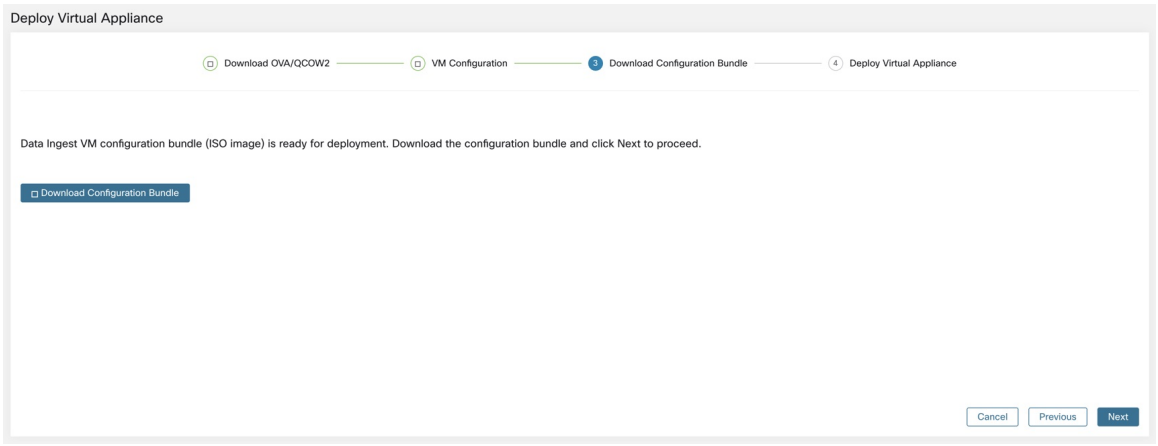


Figure 73: Deploy the VM

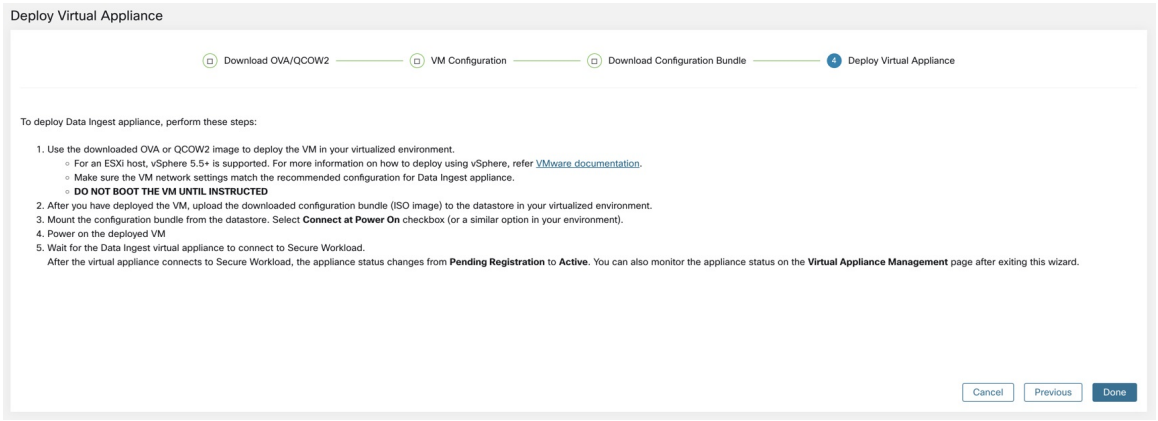
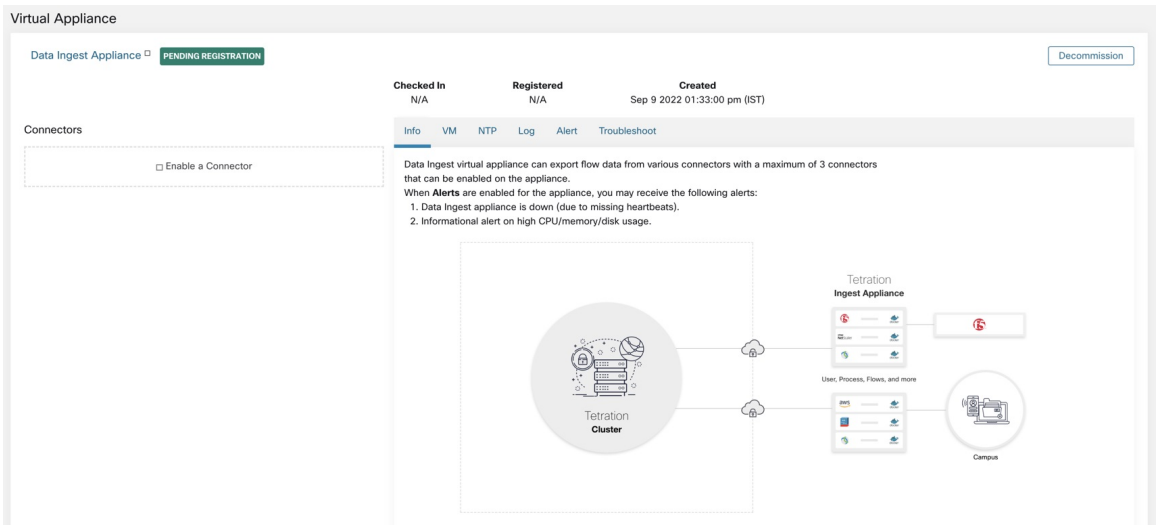


Figure 74: Cisco Secure Workload Ingest appliance in Pending Registration state



When a virtual appliance is deployed and booted up for the first time, *tet-vm-setup* service executes and sets up the appliance. This service is responsible for the following tasks

a. **Validate the appliance:** validate the appliance for mandatory resource requirements for the type of the virtual appliance deployed.

b. **IP address assignment:** assign IP addresses to all the network interfaces provisioned on the appliance.

c. **Hostname assignment:** assign hostname for the appliance (if hostname is configured).

d. **DNS configuration:** update the DNS resolv.conf file (if nameserver and/or search-domain parameters are configured).

e. **Proxy server configuration:** update HTTPS_PROXY and NO_PROXY settings on the appliance (if provided).

f. **Prepare appliance:** copies cert bundle for the Kafka topic over which appliance management messages are sent and received.

g. **Install appliance controller:** install and bring up *Appliance Controller* which is managed by *supervisord* as *tet-controller* service.

Once *tet-controller* is instantiated, it takes over the management of the appliance. This service is responsible for the following functions:

a. **Registration:** registers the appliance with Secure Workload. Until the appliance is registered, no connectors can be enabled on the appliance. When Cisco Secure Workload receives a registration request for an appliance, it updates the state of the appliance to *Active*.

b. **Deploying a connector:** deploys a connector as a Docker service on the appliance. Please refer toActivation d’un connecteur for more information.

c. **Deleting a connector:** stops and removes the Docker service and the corresponding Docker image from the appliance. Please refer to Suppression d'un connecteur for more information.

d. **Configuration updates on appliances:** tests and applies configuration updates on the appliance. Please refer to Gestion de la configuration sur les connecteurs et les appliances virtuelles for more information.

e. **Troubleshooting commands on appliances:** executes allowed set of commands on the appliances for troubleshooting and debugging issues on the appliance. Please refer to the Dépannage for more information.

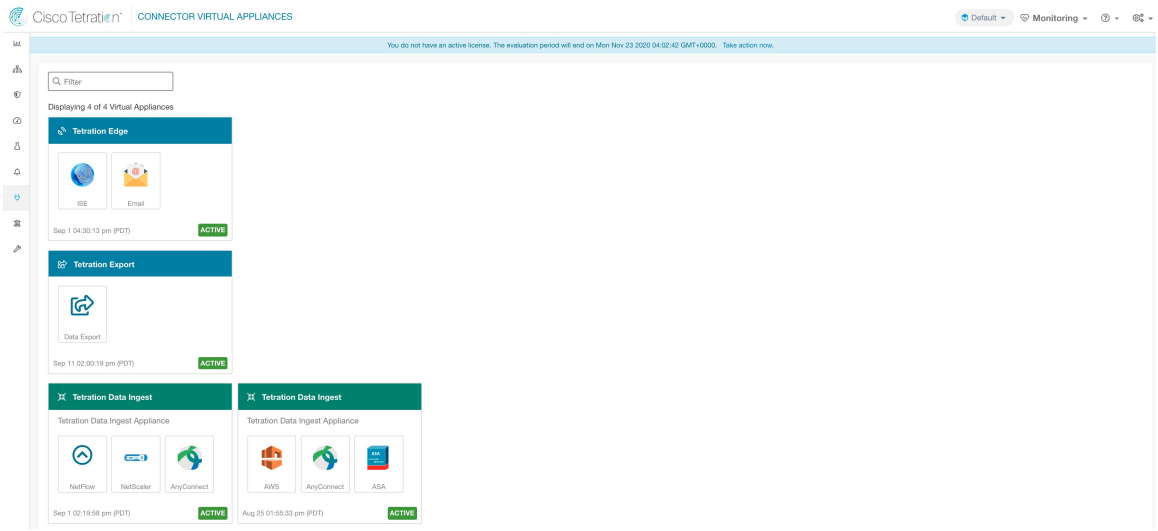
f. **Heartbeats:** periodically sends heartbeats and statistics to Cisco Secure Workload to report the health of the appliance. Please refer to Surveillance d'une appliance virtuelle for more information.

g. **Pruning:** periodically prune all Docker resources that are unused or dangling in order to recover storage space. This task is executed once every 24 hours.

h. **Decommissioning the appliance:** decommissions and deletes all Docker instances from the appliance. Please refer to Désactivation d'une appliance virtuelle for more information.

The list of deployed virtual appliances can be found at: **Manage** > **Virtual Appliances**

Figure 75: List of deployed virtual appliances



Désactivation d'une appliance virtuelle

Une appliance virtuelle peut être mise hors service dans Cisco Secure Workload. Lorsqu'une appliance est mise hors service, les actions suivantes sont déclenchées.

1. Toutes les configurations de l'appliance et les connecteurs activés sur cette dernière sont supprimés.
2. Tous les connecteurs activés sur l'appliance sont supprimés.
3. L'appliance est marquée *En attente de suppression*.
4. Lorsque l'appliance répond avec succès à la demande de suppression, le sujet et les certificats Kafka de l'appliance sont supprimés.

Note La mise hors service d'une appliance ne peut pas être annulée. Pour restaurer l'appliance et les connecteurs, une nouvelle appliance doit être déployée et les connecteurs doivent être activés sur cette dernière.

Surveillance d'une appliance virtuelle

Les appliances virtuelles Cisco Secure Workload envoient régulièrement des signaux de présence et des statistiques à Cisco Secure Workload. L'intervalle du signal de présence (heartbeat) est de 5 minutes. Les messages de signal de présence heartbeat comprennent des statistiques sur l'intégrité de l'appliance, notamment des statistiques du système, des statistiques de processus et des statistiques sur le nombre de messages envoyés, reçus ou erronés sur le sujet Kafka utilisé pour la gestion de l'appliance.

Toutes les métriques sont disponibles dans *Digger* (OpenTSDB) et sont étiquetées avec l'ID de l'appliance et le nom de la portée racine. En outre, les tableaux de bord Grafana pour le *contrôleur d'appliances* sont également disponibles pour les mesures importantes de l'appareil.

Questions de sécurité

Le système d'exploitation invité de la machine virtuelle d'acquisition/de périphérie est CentOS 7.9, dans la version logicielle de serveur/client OpenSSL qui a été supprimée. Par conséquent, la seule façon d'accéder à l'appareil est via sa console.

Note CentOS 7.9 est le système d'exploitation invité pour les appareils virtuels d'acquisition et de périphérie de Cisco Secure Workload 3.8.1.19 et les versions antérieures. À partir de la version 3.8.1.36 de Cisco Secure Workload, le système d'exploitation est AlmaLinux 9.2.

Les conteneurs exécutent une image Docker basée sur centos : 7.9.2009. La plupart des conteneurs sont exécutés avec les privilèges de base (option sans privilège), à l'exception du conteneur ERSPAN, qui a la capacité NET_ADMIN.

Note À partir de la version 3.8.1.36 de Cisco Secure Workload, les conteneurs exécutent almalinux/9-base:9.2.

Dans le cas improbable où un conteneur serait contaminé, le système d'exploitation invité de la machine virtuelle ne devrait pas pouvoir être contaminé depuis l'intérieur du conteneur.

Gestion de la configuration sur les connecteurs et les appliances virtuelles

Les mises à jour de configuration peuvent être envoyées vers les appareils et les connecteurs à partir de Cisco Secure Workload. L'appareil doit s'être enregistré avec succès auprès de Cisco Secure Workload et être *actif* avant que les mises à jour de configuration puissent être lancées. De même, les connecteurs doivent être enregistrés auprès de Cisco Secure Workload avant que les mises à jour de configuration puissent être lancées sur leurs services.

Trois modes de mise à jour de la configuration sont possibles dans les appareils et les connecteurs.

1. **Test and Apply** (Tester et appliquer) : testez la configuration et, si le test est réussi, validez-la.
2. **Discovery** (Découverte) : testez la configuration et, si le test est réussi, découvrez les propriétés supplémentaires qui peuvent être activées pour la configuration.
3. **Remove** (Supprimer) : supprimer la configuration.

Note L'appareil et le connecteur ERSPAN ne prennent pas en charge les mises à jour de configuration.

Tester et appliquer

Les configurations qui prennent en charge le mode *Test and Apply* (Tester-Appliquer) vérifient la configuration avant d'appliquer (valider) la configuration sur l'appareil et/ou le connecteur souhaité.

Configuration du protocole NTP

La configuration NTP permet à l'appareil de synchroniser l'horloge avec le ou les serveurs NTP précisés.

Nom du paramètre	Type	Description
Activer NTP	case	La synchronisation NTP doit-elle être activée?
Serveurs NTP	listof chaînes	Liste des serveurs NTP Au moins un serveur doit être indiqué et un maximum de cinq serveurs peuvent être fournis.

Test (Tester) : tester si une connexion UDP peut être établie avec les serveurs NTP donnés sur le port 123. Si une erreur se produit pour l'un des serveurs NTP, n'acceptez pas la configuration.

Apply (Appliquer) : mettez à jour `/etc/ntp.conf` et redémarrez le service ntpd à l'aide de systemctl restart ntpd.service. Voici le modèle pour générer le fichier *ntp.conf*

```
# --- GENERAL CONFIGURATION ---
server <ntp-server>
...
server 127.127.1.0
fudge 127.127.1.0 stratum 10
# Drift file
driftfile /etc/ntp/drift
```

Note Applicable à Cisco Secure Workload 3.8.1.19 et aux versions antérieures.

Pour Cisco Secure Workload 3.8.1.36 ou une version ultérieure, mettez à jour `/etc/chrony.conf` et redémarrez le service chronyd à l'aide de systemctl restart chronyd.service. Voici le modèle pour générer le fichier *chrony.conf*

```
# Secure Workload appliance chrony.conf.
server <ntp-server> iburst
...
driftfile /var/lin/chrony/drift
makestep 1.0 3
rtcsync
```

Appliances virtuelles Cisco Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 76: Erreur lors du test de la configuration NTP

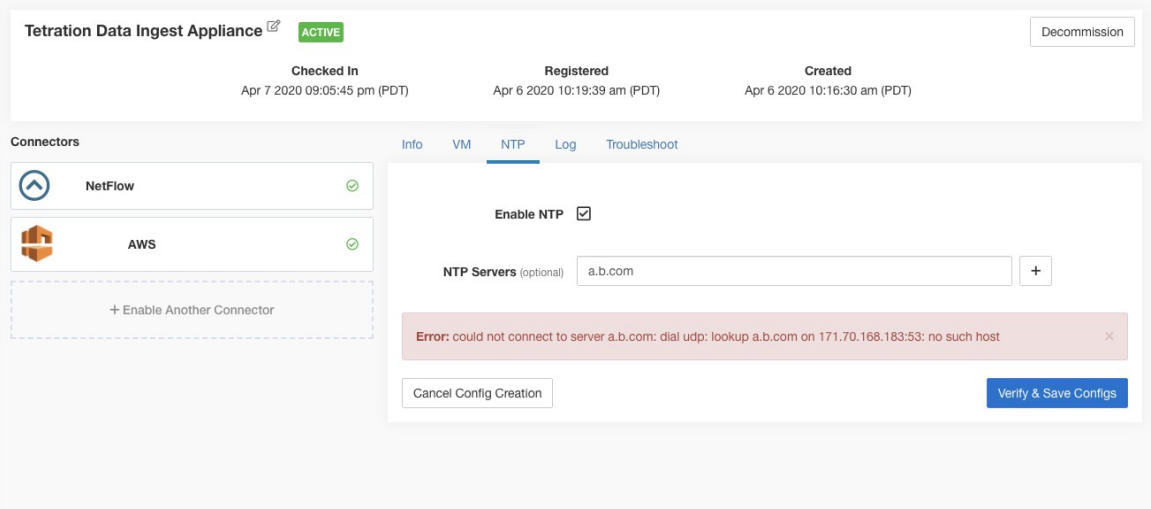


Figure 77: Configuration NTP avec des serveurs NTP valides

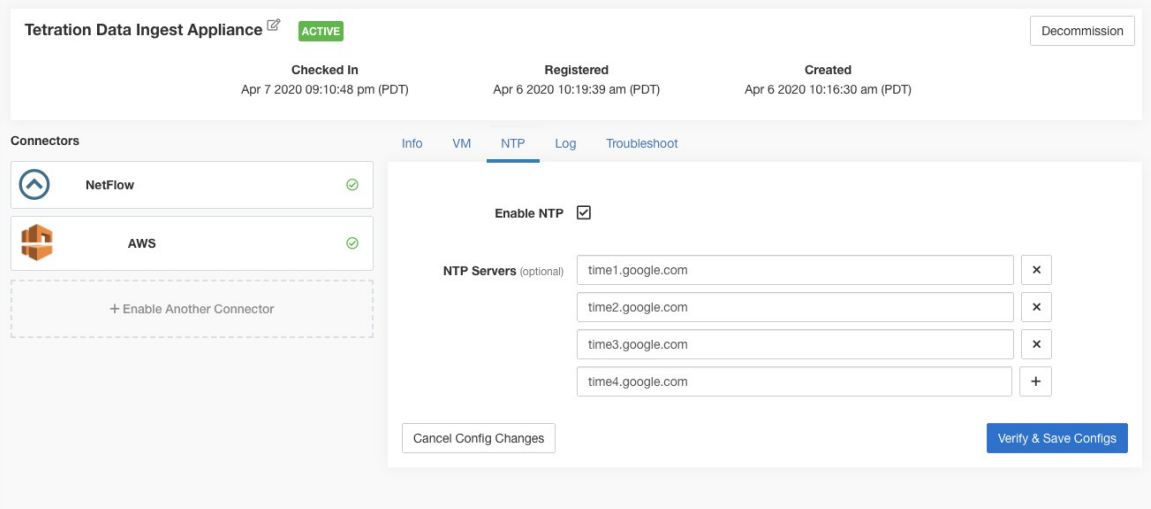
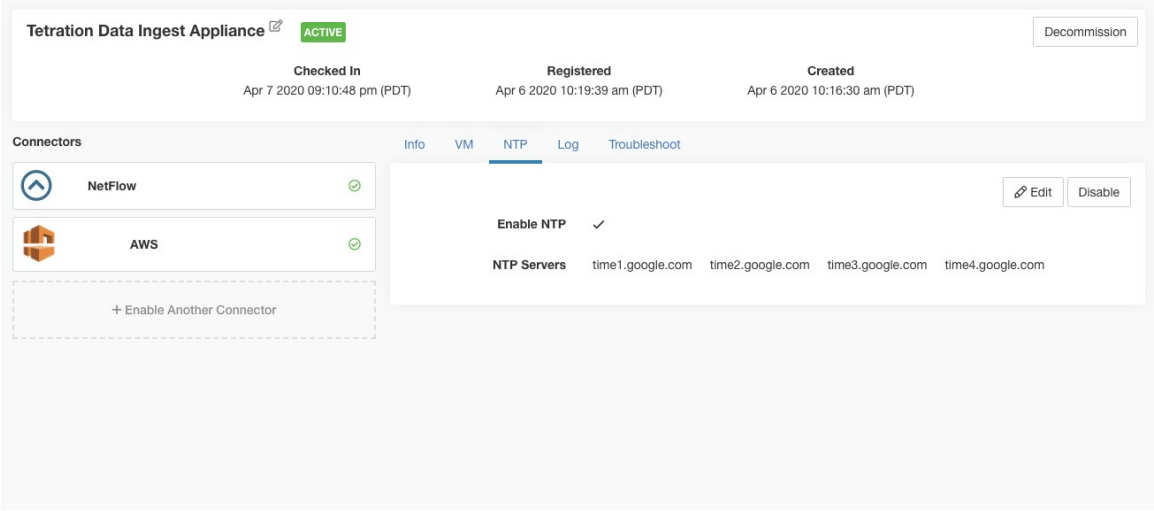


Figure 78: Configuration NTP vérifiée et appliquée



Configuration de la journalisation

La configuration des journaux met à jour les niveaux de journalisation, la taille maximale des fichiers journaux et les paramètres de rotation des journaux sur l'appareil et/ou le connecteur. Si la mise à jour de la configuration est déclenchée sur l'appareil, les paramètres du journal du contrôleur de l'appareil sont mis à jour. En revanche, si la mise à jour de la configuration est déclenchée sur un connecteur, les paramètres du contrôleur et du journal de service sont mis à jour.

Nom du paramètre	Type	Description
Niveau de journalisation	liste déroulante	Niveau de journalisation à définir
	• *débogage*	Niveau de journal de débogage
	• *Information*	Niveau de journalisation informatif
	• *avertir*	Niveau du journal des avertissements
	• *erreur*	Niveau du journal des erreurs
Taille maximale du fichier journal (en Mo)	number	Taille maximale d'un fichier de journal avant le début de la rotation des journaux
Rotation des journaux (en jours)	number	Longévité maximale d'un fichier journal avant le début de la rotation des journaux
Rotation des journaux (dans les instances)	number	Nombre maximal d'instances de fichiers journaux conservées

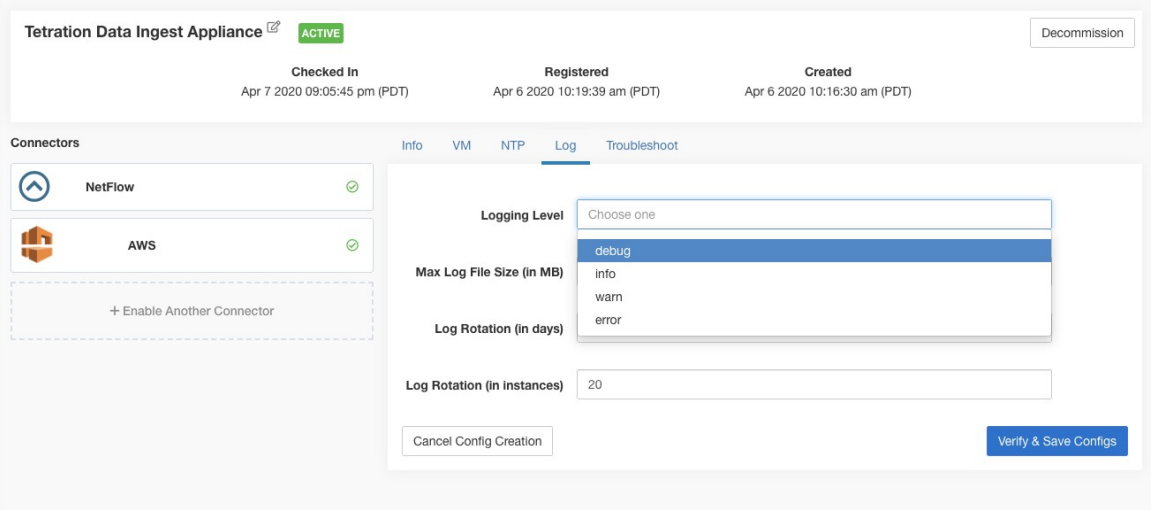
Test : pas d'opération

Apply (Appliquer) : Si la configuration est déclenchée sur un appareil, mettez à jour le fichier de configuration de *tet-controller* sur l'appareil. Si la configuration est déclenchée sur un connecteur, mettez à jour les fichiers de configuration de *tet-controller* et le service géré par le contrôleur sur le conteneur Docker responsable du connecteur.

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, ISE, ASA et Meraki.

Figure 79: Configurer le journal sur l'appareil



Note Comme tous les connecteurs de notification d'alerte (Syslog, Courriel, Slack, PagerDuty et Kinesis) fonctionnent sur un seul service Docker (Secure Workload Alert Alert Notifier) sur Cisco Secure Workload Edge, il n'est pas possible de mettre à jour la configuration du journal d'un connecteur sans avoir une incidence sur la configuration d'un autre connecteur de notification d'alerte. Les configurations des journaux du service Docker Cisco Secure Workload Alert Notifier (TAN) sur l'appareil de périphérie Cisco Secure Workload peuvent être mises à jour à l'aide d'une commande autorisée.

Consultez la section Mettre à jour la configuration des journaux du connecteur de l'outil de notification d'alerte pour de plus amples renseignements.

Configuration du point terminal

La configuration de point terminal précise le délai d'inactivité des points terminaux sur les connecteurs AnyConnect et ISE. Lorsqu'un point terminal expire, le connecteur arrête de s'enregistrer auprès de Cisco Secure Workload et purge l'état local du point terminal sur le connecteur.

Nom du paramètre	Type	Description
Délai d'expiration d'inactivité pour les points terminaux (en minutes)	number	Délai d'inactivité pour les points terminaux publiés par les connecteurs AnyConnect et ISE. À l'expiration du délai, le point terminal ne procédera plus à l'enregistrement de Cisco Secure Workload. (Valeur par défaut : 30 minutes).

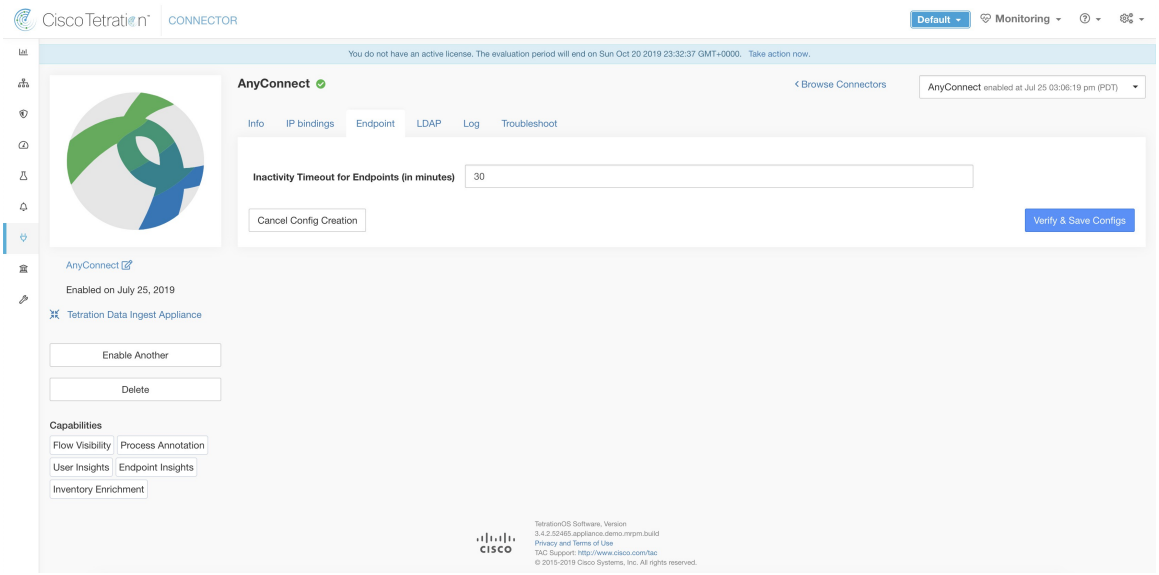
Test : pas d'opération

Apply (Appliquer) : mettez à jour le fichier de configuration du connecteur avec la nouvelle valeur

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : AnyConnect et ISE

Figure 80: Configuration du délai d'inactivité des points terminaux sur le connecteur AnyConnect



Configuration de l'outil de notification Slack

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur Slack.

Nom du paramètre	Type	Description
URL de point d'ancrage Web Slack	chaîne	Point d'ancrage Web Slack sur lequel les alertes Cisco Secure Workload doivent être publiées

Test(Tester) : envoyez une alerte de test à Slack à l'aide du point d'ancrage Web. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : Slack

Configuration de l'outil de notification PagerDuty

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur PagerDuty.

Nom du paramètre	Type	Description
Clé de service PagerDuty	chaîne	Clé de service PagerDuty pour l'envoi des alertes de Cisco Secure Workload sur PagerDuty

Test : permet d'envoyer une alerte de test à PagerDuty à l'aide de la clé de service. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : PagerDuty

Configuration de l'outil de notification Kinesis

Configuration par défaut pour la publication des alertes Cisco Secure Workload sur Amazon Kinesis.

Nom du paramètre	Type	Description
ID de la clé d'accès AWS	chaîne	ID de clé d'accès AWS pour communiquer avec AWS
Clé d'accès secrète AWS	chaîne	Clé d'accès secrète AWS pour communiquer avec AWS
Région AWS	dropdown of AWS regions	Nom de la région AWS où le flux Kinesis est configuré
Kinesis Stream	chaîne	Nom du flux Kinesis
Stream Partition	chaîne	Nom de la partition du flux

Test (Tester) : envoie une alerte de test au flux Kinesis en utilisant la configuration donnée. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : Kinesis

Configuration de l'outil de notification des courriels

Configuration par défaut pour la publication des alertes Cisco Secure Workload dans un courriel.

Nom du paramètre	Type	Description
Nom d'utilisateur SMTP	chaîne	Nom d'utilisateur du serveur SMTP Ce paramètre est facultatif.
Mot de passe SMTP	chaîne	Mot de passe du serveur SMTP pour l'utilisateur (si fourni) Ce paramètre est facultatif.
SMTP Server	chaîne	Nom d'hôte ou adresse IP du serveur SMTP
Port SMTP	number	Port d'écoute du serveur SMTP. La valeur par défaut est 587.
Connection sécurisée	case	Doit-on utiliser SSL pour la connexion au serveur SMTP?
Adresse courriel d'expédition	chaîne	Adresse courriel à utiliser pour l'envoi des alertes
Destinataires par défaut	chaîne	Liste d'adresses courriel de destinataires séparées par des virgules

Test : envoyez un courriel de test en utilisant la configuration fournie. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : courriel

Configuration de l'outil de notification Syslog

Configuration par défaut pour la publication des alertes Cisco Secure Workload dans Syslog.

Nom du paramètre	Type	Description
Protocol	liste déroulante	Protocole à utiliser pour la connexion au serveur
	•*UDP*	
	• *TCP*	
Adresse du serveur	chaîne	Nom d'hôte ou adresse IP du serveur Syslog.
Port	number	Port d'écoute du serveur Syslog. La valeur du port par défaut est 514.

Test (Tester): envoie une alerte de test au serveur Syslog en utilisant la configuration donnée. Si l'alerte est publiée avec succès, le test est réussi.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : syslog

Configuration du mappage de gravité Syslog

Le tableau suivant présente le mappage de gravité par défaut pour les alertes Cisco Secure Workload dans Syslog.

Gravité des alertes pour Cisco Secure Workload	Gravité de journal système
FAIBLE	LOG_DEBUG
MOYENNE	LOG_WARNING
ÉLEVÉE	LOG_ERR
CRITIQUE	JOURNAL_CRIT
ACTION IMMÉDIATE	LOG_EMERG

Vous pouvez modifier ce paramètre à l'aide de cette configuration.

Nom du paramètre	Liste déroulante des mappages
ACTION_IMMÉDIATE	• *Urgence* • *Alerte* • *Critique* • *Erreur* • *Avertissement* • *Avis* • *Information* • *Débogage*
CRITIQUE	
ÉLEVÉ	
MOYENNE	
FAIBLE	

Test : pas d'opération

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : syslog

Configuration de l'instance ISE

Cette configuration fournit les paramètres nécessaires pour la connexion à Cisco Identity Services Engine (ISE). En fournissant plusieurs instances de cette configuration, le connecteur ISE peut se connecter et extraire les métadonnées concernant les points terminaux de plusieurs appareils ISE. Jusqu'à 20 instances de configuration ISE peuvent être fournies.

Nom du paramètre	Type	Description
Certificat client ISE	chaîne	Certificat client ISE pour se connecter à ISE à l'aide de pxGrid
Clé de client ISE	chaîne	Clé client ISE pour se connecter à ISE
Certificat de l'autorité de certification du serveur ISE	chaîne	Certificat de l'autorité de certification ISE
Nom d'hôte ISE	chaîne	Nom de domaine complet de ISE pxGrid
Nom de nœud ISE	chaîne	Nom de nœud de ISE pxGrid

Test (Test) : connectez-vous à ISE en utilisant les paramètres fournis. Une fois la connexion réussie, acceptez la configuration.

Apply(Appliquer) : Mettre à jour le fichier de configuration du connecteur avec les paramètres spécifiés.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : ISE

Découverte

Les configurations qui prennent en charge le mode *découverte* effectuent ce qui suit.

1. Obtenir une configuration de base auprès de l'utilisateur.
2. Vérifier configuration de base.
3. Détecter les propriétés supplémentaires de la configuration et les présenter à l'utilisateur.
4. Laissez l'utilisateur améliorer la configuration à l'aide des propriétés découvertes.
5. Vérifier et appliquer la configuration améliorée.

Dans la version 3.3.1.x, la configuration LDAP prend en charge le mode de découverte.

Configuration LDAP

La configuration LDAP précise comment se connecter au LDAP, quel est le nom distinctif (DN) de base à utiliser, quel est l'attribut qui correspond au nom d'utilisateur et quels attributs récupérer pour chaque nom d'utilisateur. Les attributs LDAP sont des propriétés de LDAP qui sont spécifiques à cet environnement.

Compte tenu de la configuration de la connexion à LDAP et du DN de base, il est possible de découvrir les attributs des utilisateurs dans LDAP. Ces attributs détectés peuvent ensuite être présentés à l'utilisateur dans l'interface utilisateur. Parmi ces attributs découverts, l'utilisateur sélectionne l'attribut qui correspond au nom d'utilisateur et une liste de six attributs maximum à collecter pour chaque nom d'utilisateur à partir de LDAP. Par conséquent, cela rend inutile la configuration manuelle des attributs LDAP et réduit les erreurs.

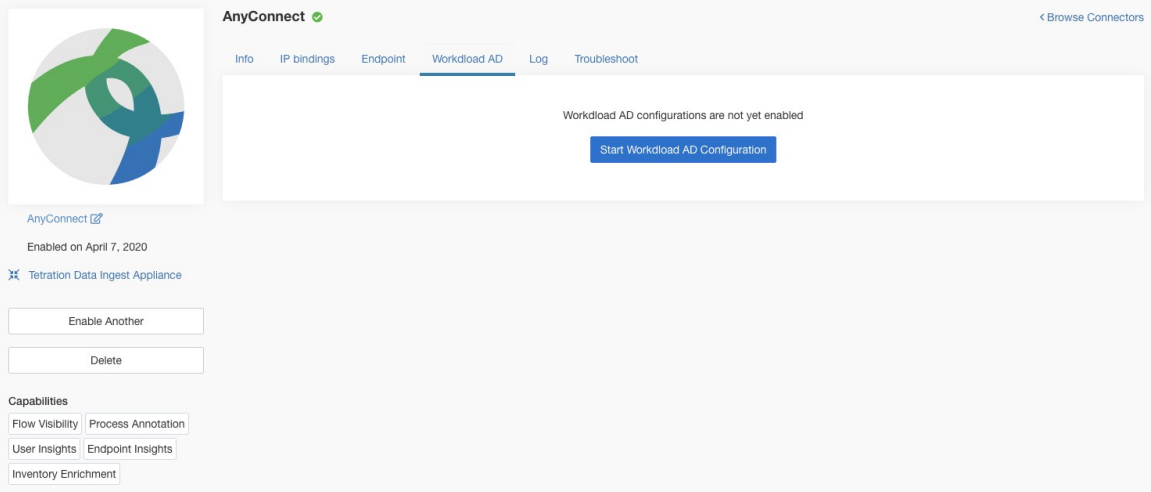
Voici les étapes détaillées de la création d'une configuration LDAP par découverte.

Procedure

Étape 1 Commencez la configuration LDAP

Lancez une configuration LDAP pour le connecteur.

Figure 81: Démarrez la découverte de la configuration LDAP



Étape 2 Fournissez une configuration LDAP de base

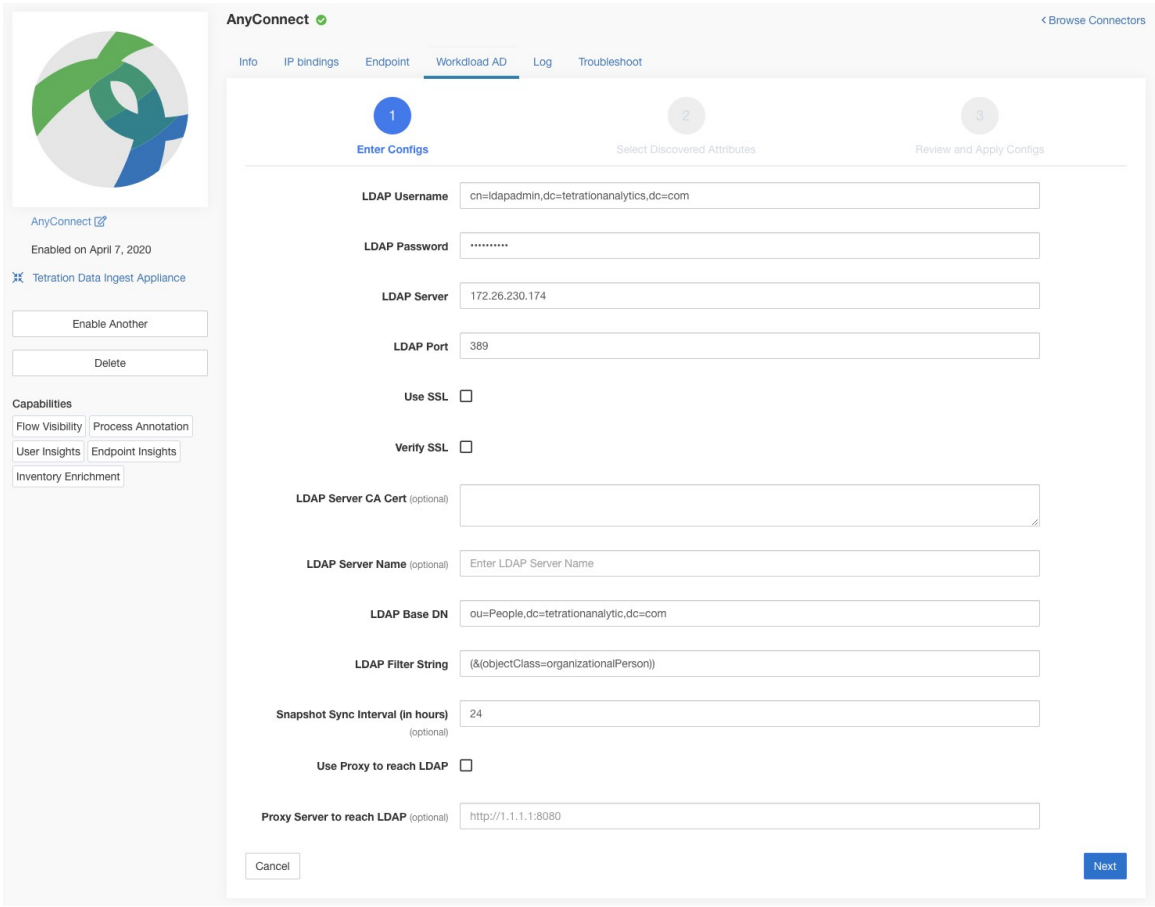
Précisez la configuration de base pour la connexion à LDAP. Dans cette configuration, les utilisateurs fournissent le DN de liaison LDAP ou le nom d'utilisateur pour la connexion au serveur LDAP, le mot de passe LDAP à utiliser pour la connexion au serveur LDAP, l'adresse du serveur LDAP, le port du serveur LDAP, le DN de base auquel se connecter et une chaîne de filtre pour récupérer les utilisateurs qui correspondent à ce fichier.

Nom du paramètre	Type	Description
Nom d'utilisateur LDAP	chaîne	Nom d'utilisateur LDAP ou DN de liaison pour accéder au serveur LDAP*
LDAP Password	chaîne	Mot de passe LDAP pour le nom d'utilisateur pour accéder au serveur LDAP*
LDAP Server	chaîne	Adresse du serveur LDAP
Port LDAP	number	Port du serveur LDAP
Utiliser le protocole SSL	case	Le connecteur doit-il se connecter à LDAP de manière sécurisée? Facultatif. La valeur par défaut est False.

Nom du paramètre	Type	Description
Verify SSL	case	Le connecteur doit-il vérifier le certificat LDAP? Facultatif. La valeur par défaut est False.
LDAP Server CA Cert	chaîne	Certificat de l'autorité de certification du serveur Facultatif.
Nom du serveur LDAP	chaîne	Nom du serveur pour lequel le certificat LDAP est émis (obligatoire si la case *Vérifier SSL* est cochée.
DN de base LDAP	chaîne	DN de base LDAP, le point de départ des recherches dans l'annuaire dans LDAP
LDAP Filter String	chaîne	Chaîne de préfixe de filtre LDAP Filtrez les résultats de la recherche qui correspondent uniquement à cette condition.
Snapshot Sync Interval (in hours)	number	Spécifiez l'intervalle de temps en heures pour (re)créer un instantané LDAP. Facultatif. Le réglage par défaut est de 24 heures.
Utiliser un serveur mandataire pour accéder à LDAP	case	Le connecteur doit-il utiliser un serveur mandataire pour accéder au serveur LDAP?
Serveur mandataire pour accéder à LDAP	chaîne	Serveur serveur mandataire pour accéder à LDAP

Les autorisations utilisateur minimales nécessaires pour configurer LDAP sur les connecteurs sont un **Utilisateur de domaine standard**.

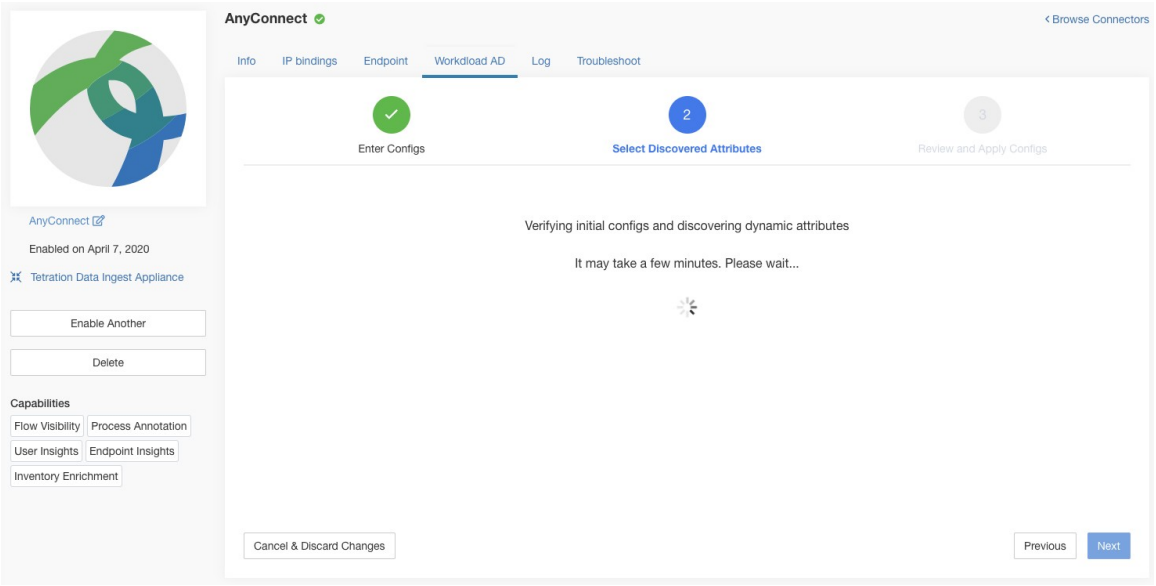
Figure 82: Configuration initiale LDAP



Étape 3 Découverte en cours

Une fois que l'utilisateur a cliqué sur *Next* (suivant), cette configuration est envoyée au connecteur. Le connecteur établit une connexion avec le serveur LDAP en utilisant la configuration fournie. Il récupère jusqu'à 1 000 utilisateurs du serveur LDAP et identifie tous les attributs. En outre, il calcule une liste de tous les attributs à valeur unique communs aux 1 000 utilisateurs. Le connecteur renvoie ce résultat à Cisco Secure Workload.

Figure 83: Découverte en cours



Étape 4 **Améliorez la configuration avec les attributs découverts**

L'utilisateur doit choisir l'attribut correspondant au nom d'utilisateur et sélectionner jusqu'à six attributs que le connecteur doit récupérer et enregistrer pour chaque utilisateur de de l'organisation (c'est-à-dire les utilisateurs correspondant à la chaîne de filtrage). Cette action est effectuée à l'aide d'une liste déroulante d'attributs détectés. Ainsi, vous éliminez les erreurs manuelles et les erreurs de configuration.

Nom du paramètre	Type	Description
Attribut de nom d'utilisateur LDAP	chaîne	Attribut LDAP qui contient le nom d'utilisateur
Attributs LDAP à récupérer	liste de chaînes	Liste des attributs LDAP qui doivent être extraits pour un utilisateur

Figure 84: Détecter les attributs LDAP

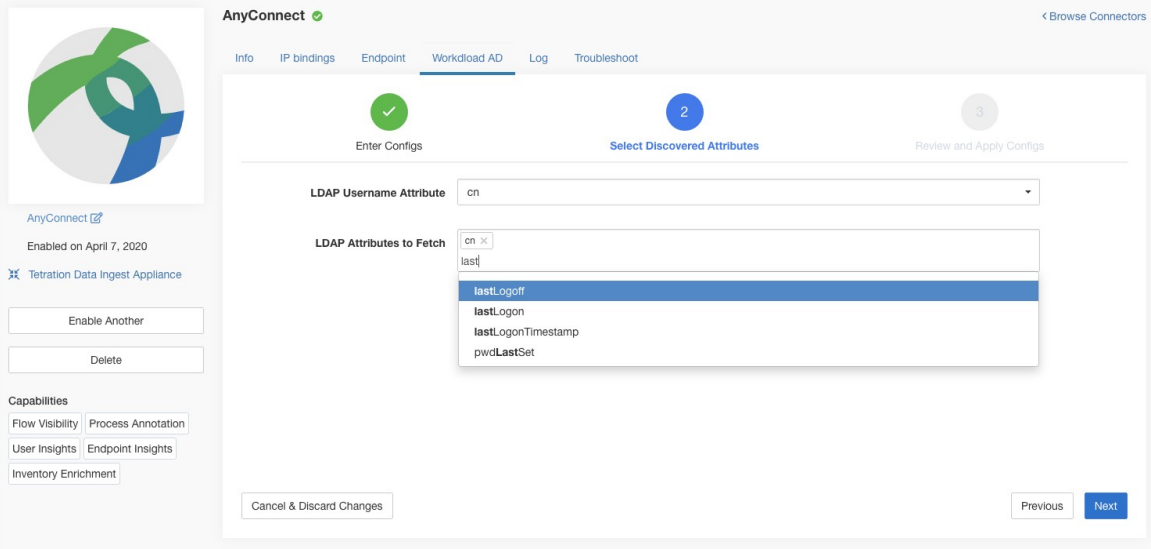
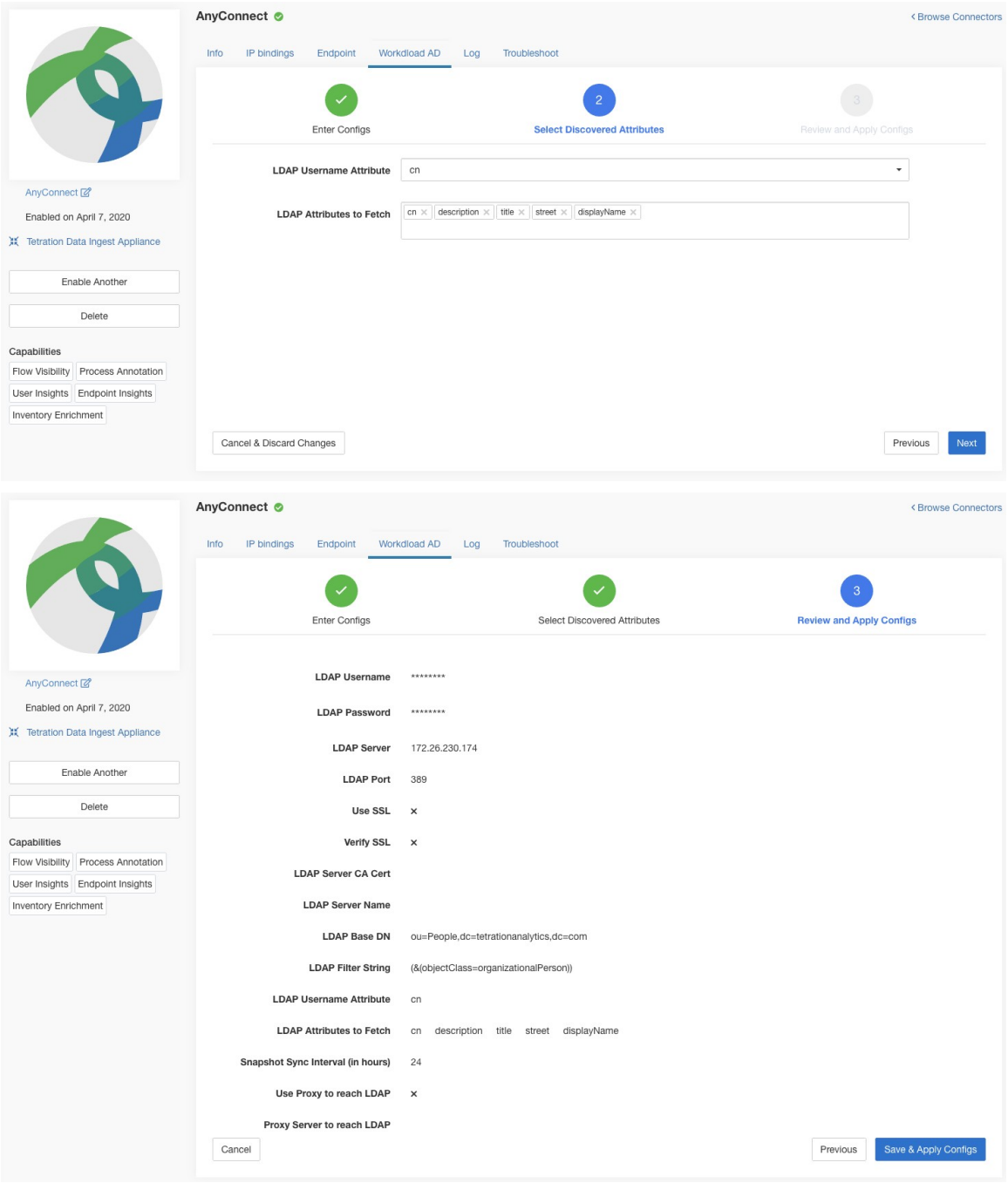


Figure 85: Déterminer l'attribut de nom d'utilisateur et les attributs à recueillir pour chaque nom d'utilisateur

Étape 5 Finaliser, enregistrer et appliquer la configuration

Enfin, la configuration est terminée en cliquant sur *Save and Apply Changes*(enregistrer et appliquer les modifications).

Figure 86: Terminer la découverte et la validation de la configuration LDAP



Le connecteur reçoit la configuration terminée. Il crée un instantané local de tous les utilisateurs correspondant à la chaîne de filtre et récupère uniquement les attributs sélectionnés. Une fois la prise d'instantané terminée, les services du connecteur peuvent commencer à utiliser l'instantané pour annoter les utilisateurs et leurs attributs LDAP dans les inventaires.

Appliances virtuelles Cisco Secure Workload autorisées : Aucune

Connecteurs autorisés : AnyConnect, ISE et F5.

Supprimer

Vous pouvez supprimer toutes les configurations que vous avez ajoutées des connecteurs ou des appareils en utilisant le bouton *Delete* (Supprimer) disponible pour chaque configuration.

Dépannage

Les connecteurs et les appliances virtuelles prennent en charge divers mécanismes de dépannage pour déboguer les problèmes éventuels.

Note La présente section ne s'applique pas aux éléments suivants :

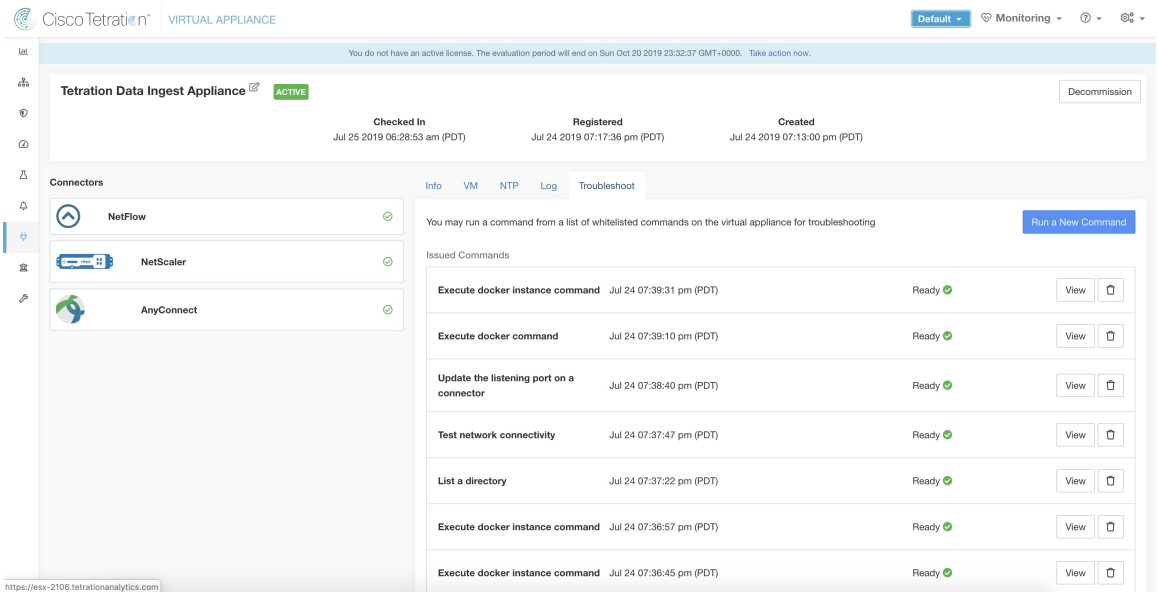
Appliance virtuelle ERSPAN : reportez-vous à la page de l'appliance ERSPAN pour en savoir plus sur le dépannage.

Connecteurs infonuagiques : pour dépanner les connecteurs infonuagiques, consultez la section de votre connecteur infonuagique, par exemple Résoudre les problèmes de connecteur AWS.

Ensemble de commandes autorisé

L'ensemble de commandes autorisé vous permet d'exécuter certaines commandes de débogage sur les appareils et les conteneurs Docker (pour les connecteurs). Les commandes autorisées comprennent la possibilité de récupérer les journaux et la configuration d'exécution actuelle, de tester la connectivité réseau et de capturer des paquets correspondant à un port spécifié.

Figure 87: Page de dépannage sur l'appliance virtuelle Cisco Secure Workload



Note Le dépannage à l'aide de l'ensemble de commandes autorisé est disponible sur les périphériques et les connecteurs uniquement pour les utilisateurs ayant le rôle *Service à la clientèle*.

Afficher les journaux

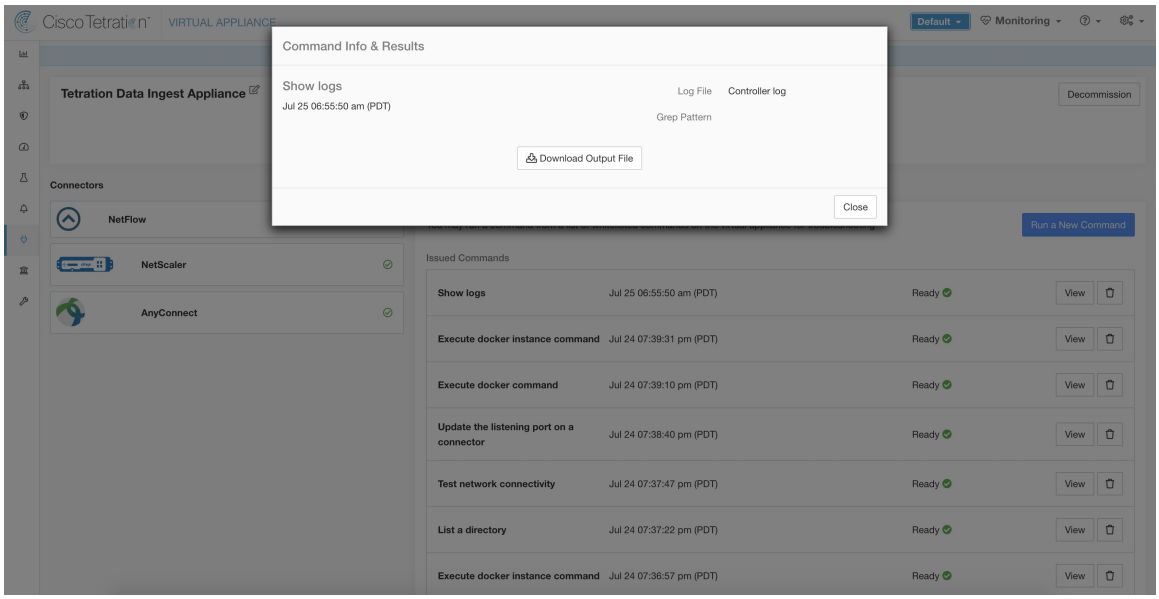
Affiche le contenu d'un fichier journal de contrôleur et permet éventuellement de traiter le fichier selon un modèle précisé. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Lorsque le résultat est disponible dans Cisco Secure Workload, un bouton de téléchargement s'affiche permettant de télécharger le fichier.

Nom de l'argument	Type	Description
Modèle Grep	chaîne	Chaîne de schéma Grep dans le fichier journal

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 88: Télécharger la sortie d'affichage des journaux à partir de l'appareil d'acquisition Cisco Secure Workload



Afficher les journaux de service

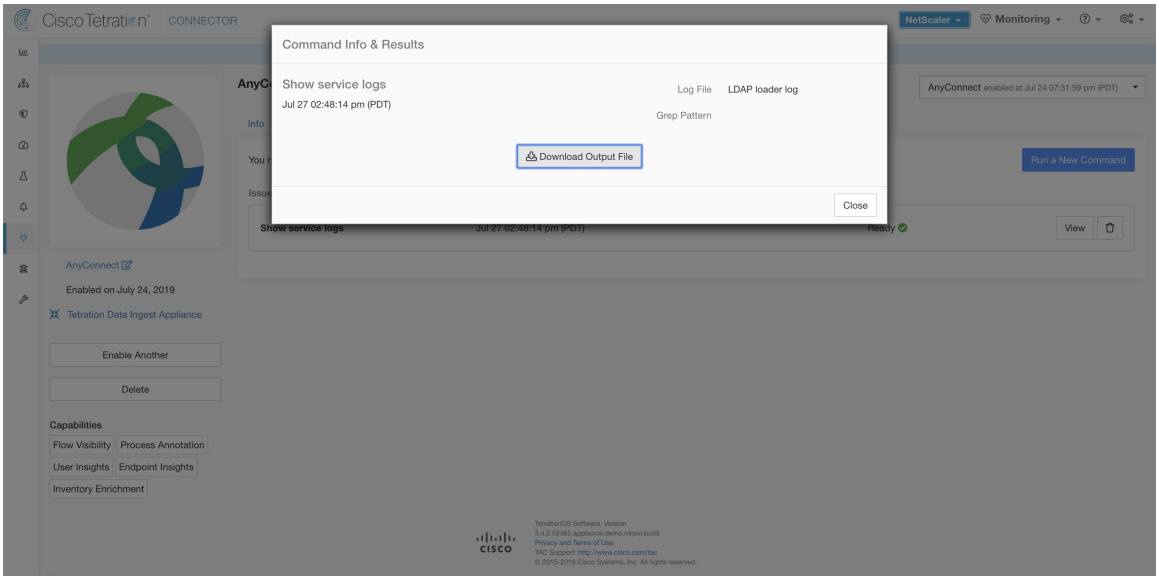
Affiche le contenu des fichiers journaux de service et permet éventuellement de saisir le fichier selon un modèle spécifié. Cisco Secure Workload envoie la commande à l'appareil/au connecteur sur lequel la commande a été exécutée. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Lorsque le résultat est disponible dans Cisco Secure Workload, un bouton de téléchargement s'affiche permettant de télécharger le fichier.

Nom de l'argument	Type	Description
Log File	liste déroulante	Le nom du fichier journal à collecter
	• *Service log*	Journaux du service du connecteur
	• *Upgrade log*	Journaux de mise à niveau du service
	• *LDAP loader log*	Journaux de l'instantané LDAP pour les connecteurs pour lesquels LDAP est activé
Modèle Grep	chaîne	Chaîne de schéma Grep dans le fichier journal

Appliances virtuelles Cisco Secure Workload autorisées : aucune (disponible uniquement avec les services de connecteur valides)

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 89: Téléchargez la sortie d'affichage des journaux de service du connecteur AnyConnect pour le fichier de journalisation du chargeur LDAP



Afficher la configuration d'exécution

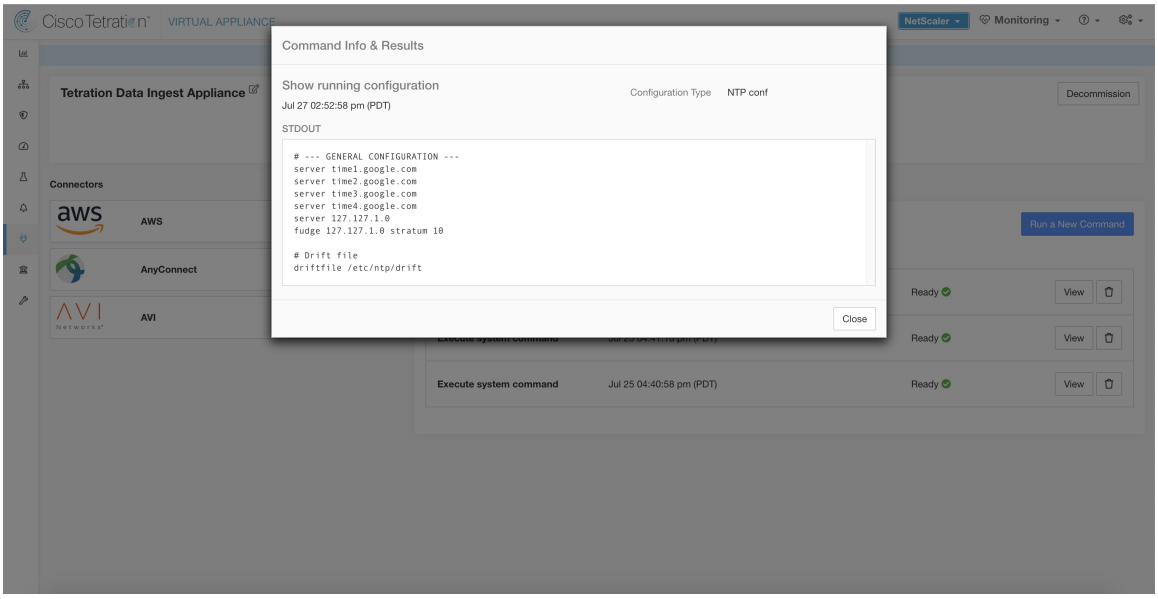
Afficher la configuration en cours d'exécution d'un appareil ou des contrôleurs de connecteur. Le contrôleur de l'appareil ou du connecteur récupère la configuration correspondant à l'argument demandé et renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, le contenu de la configuration s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Type de configuration	liste déroulante	Fichier de configuration à recueillir
	• *Configuration du contrôleur*	Fichier de configuration du contrôleur de l'appareil
	• *Configuration du superviseur*	Fichier de configuration du superviseur qui exécute le contrôleur
	• *Configuration NTP*	Fichier de configuration NTP
	• *Conférence Chrony*	/etc/chrony.conf

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 90: Afficher la configuration en cours d'exécution pour la conférence NTP sur un appareil d'acquisition Cisco Secure Workload



Afficher la configuration d'exécution du service

Affichez la configuration en cours d'exécution des services instanciés pour les connecteurs sur les appareils. Le contrôleur du service récupère la configuration correspondant à l'argument demandé et renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, le contenu de la configuration s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Type de configuration	liste déroulante	Fichier de configuration à recueillir.
	• *Configuration du contrôleur*	Fichier de configuration du contrôleur de service.
	• *Configuration du superviseur*	Fichier de configuration du superviseur qui exécute le contrôleur.
	• *Configuration de service*	Fichier de configuration du service.
	• *Configuration LDAP*	Configuration LDAP pour les connecteurs pour lesquels LDAP est activé.

Appliances virtuelles Cisco Secure Workload autorisées : aucune (disponible uniquement avec les services de connecteur valides)

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Afficher les commandes système

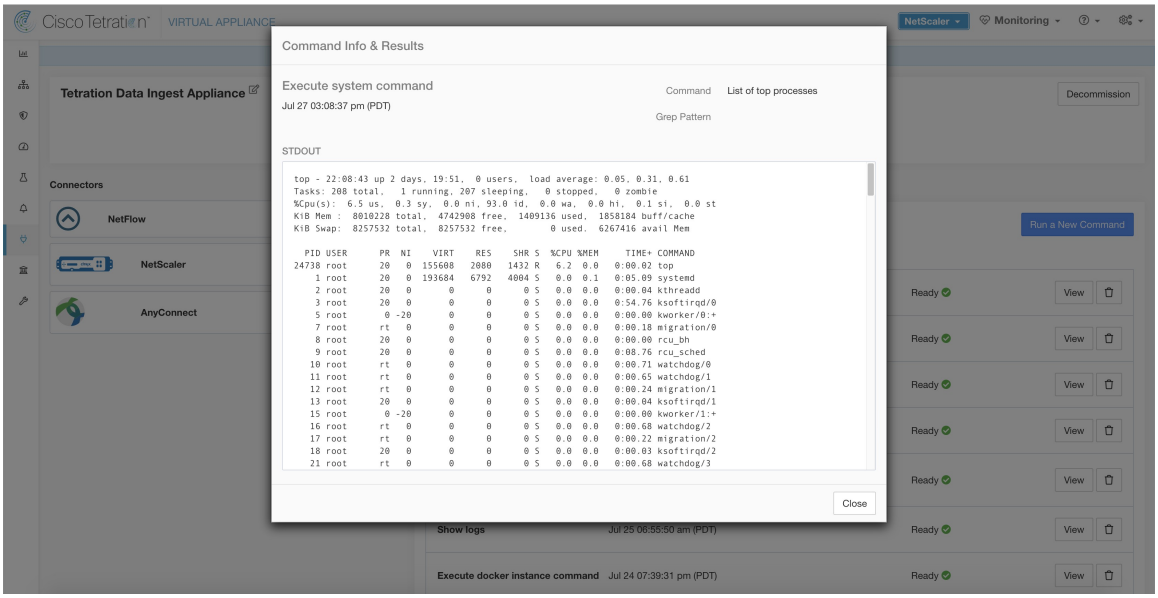
Exécutez une commande système et éventuellement grep pour un modèle spécifié. Le contrôleur du service de l'appareil/du connecteur renvoie le résultat (avec les 5000 dernières lignes). Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commandes système	liste déroulante	Commande système à exécuter
	• *Configuration IP*	**ifconfig**
	• *Configuration de la route IP*	**ip route**
	• *Règles de filtrage de paquets IP*	**iptables -L**
	• *État du réseau*	**netstat**
	• *État du réseau (EL9)*	**ss**
	• *État du processus*	**ps -aux**
	• *Liste des principaux processus*	**top -b -n 1**
	• *État NTP*	**ntpstat**
	• *Requête NTP*	**ntpq -pn**
	• État Chrony (EL9)	**suivi Chronyc**
	• Requête Chrony (EL9)	**sources chronyc**
	• *Informations sur le processeur*	**lscpu**
	• *Informations sur la mémoire*	**lsmem**
	• *Disque libre*	**df -H**
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 91: Afficher la commande système sur l'appareil d'acquisition Cisco Secure Workload pour récupérer la liste des principaux processus



Afficher les commandes Docker

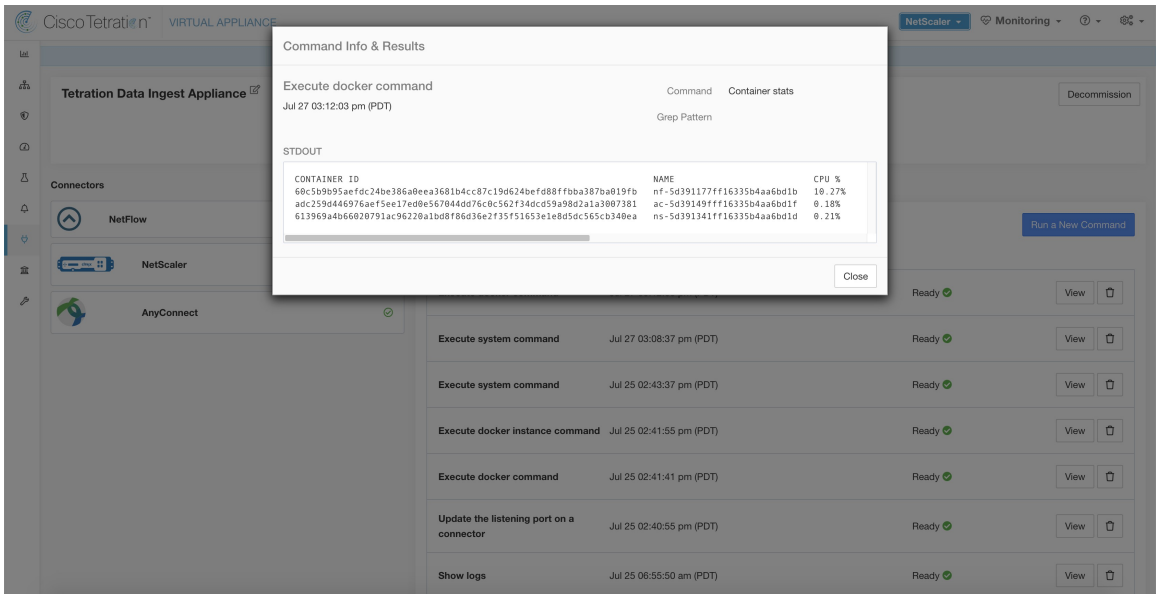
Exécutez une commande Docker et éventuellement grep pour un modèle spécifié. La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Le résultat s'est arrêté aux 5000 dernières lignes. Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande Docker	liste déroulante	Commande Docker à exécuter
	• *Docker info*	**Renseignements sur Docker**
	• *List images*	**images de Docker --non tronquées**
	• *List containers*	**Docker ps --non tronqués**
	• *List networks*	**réseau docker est --non tronqué**
	• *List volumes*	**volume Docker est**
	• *Statistiques des conteneurs*	**Statistiques de Docker –non tronquées - aucun flux**
	• *Utilisation du disque Docker*	`docker system df -v`
	• *Événements du système Docker*	**Événements système Docker --depuis '10m'**
	• *Version*	**version de Docker**
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 92: Exécutez une commande Docker sur l'appareil d'acquisition Cisco Secure Workload pour afficher les statistiques du conteneur



Afficher les commandes d'instance Docker

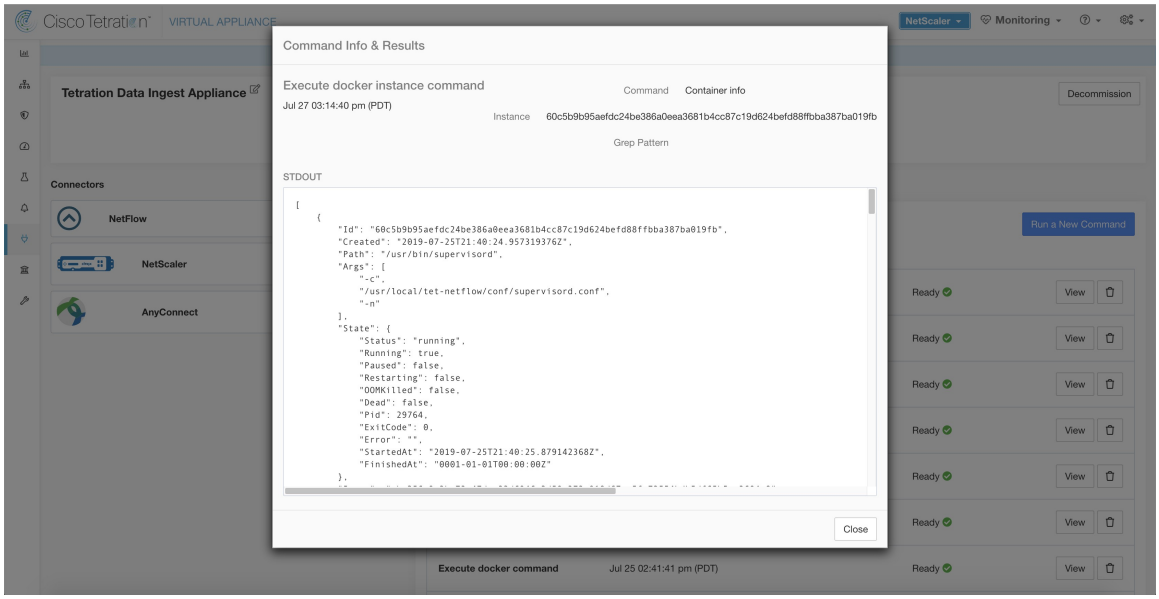
Exécutez une commande Docker sur une instance spécifique d'une ressource Docker. L'ID d'instance peut être récupéré à l'aide de l'option Afficher les commandes Docker (Afficher les commandes Docker). La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Le résultat s'est arrêté aux 5000 dernières lignes. Si vous le souhaitez, un modèle grep peut être fourni en tant qu'argument et la sortie est filtrée en conséquence. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande Docker	liste déroulante	Commande Docker à exécuter
	• *Informations sur l'image*	**images de Docker --non tronquées <instance>**
	• *Informations sur le réseau*	**inspection du réseau de Docker<instance>**
	• *Informations sur le volume*	**Inspecter le volume Docker<instance>**
	• *Informations sur le conteneur*	**Docker conteneur inspect--taille<instance>**
	• *Journaux des conteneurs*	**Journaux Docker --derniers 5000<instance>**
	• *Mappages de ports de conteneur*	**port Docker<instance>**
	• *Statistiques d'utilisation des ressources du conteneur*	**Statistiques Docker –non tronquée--aucun flux<instance>**
	• *Processus en cours d'exécution de conteneur*	**docker top <instance>**
Instance	chaîne	ID de ressource Docker (image, réseau, volume, conteneur) (voir Afficher les commandes Docker)
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 93: Exécutez une commande d'instance Docker sur l'appareil d'acquisition Cisco Secure Workload pour récupérer les informations sur le conteneur



Afficher les commandes du superviseur

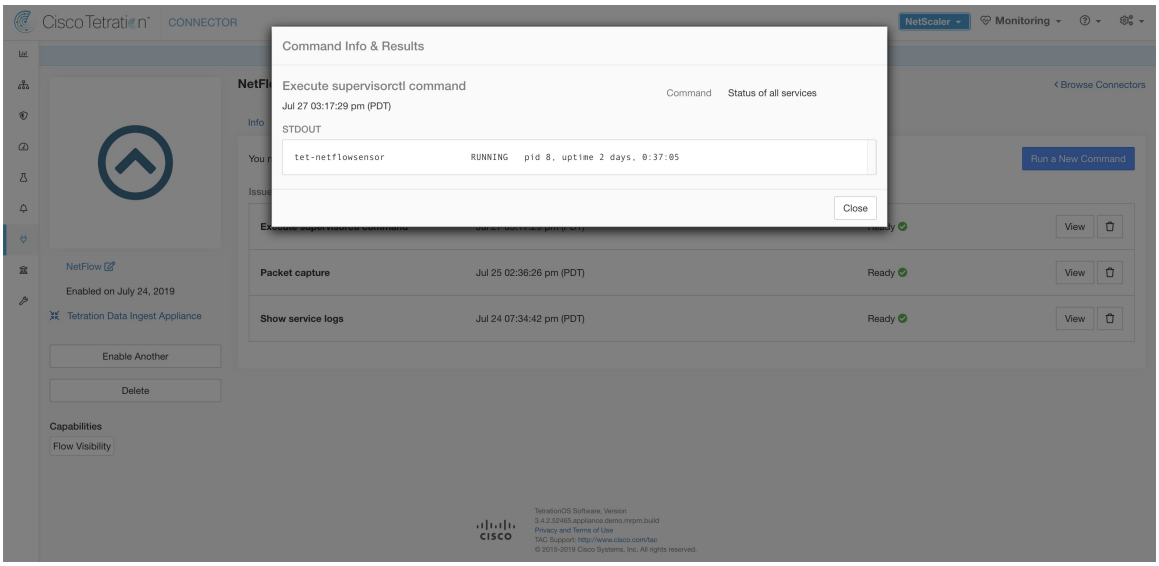
Exécutez une commande supervisorctl et renvoyez le résultat. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur sur le dispositif ou le service du connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il s'affiche dans une zone de texte.

Nom de l'argument	Type	Description
Commande SupervisorCtl	liste déroulante	commande *supervisorctl* à exécuter
	• *État de tous les services*	**supervisorctl status**
	• *PID du superviseur*	**supervisorctl pid all**
	• *PID de tous les services*	**supervisorctl pid all**

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 94: Exécutez la commande supervisorctl sur le connecteur NetFlow pour obtenir l'état de tous les services

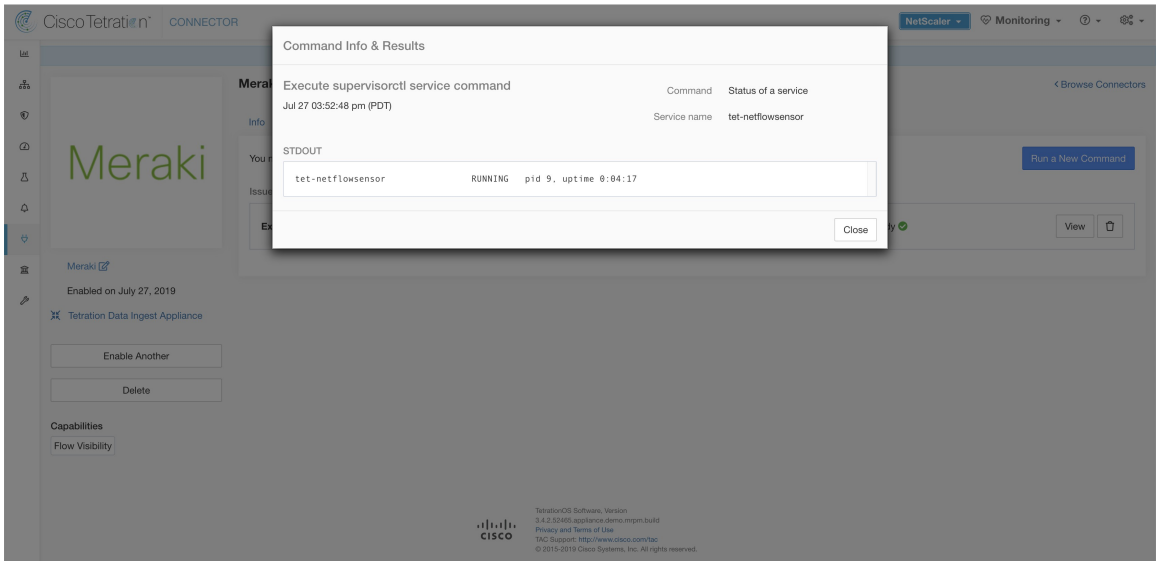


Afficher les commandes de service du superviseur

Exécutez une commande supervisorctl pour un service spécifique. Le nom du service peut être récupéré à l'aide Afficher les commandes du superviseur(afficher le superviseur). Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été émise. Le contrôleur service de l'appareil/du connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande SupervisorCtl	liste déroulante	commande *supervisorctl* à exécuter
	• *État d'un service*	**supervisorctl status <nom du service>**
	• *PID d'un service*	**supervisorctl pid <nom du service>**
Service name	chaîne	Nom du service contrôlé par le superviseur (voir la section Afficher les commandes du superviseur)

Figure 95: Exécutez la commande supervisorctl sur le connecteur NetFlow pour obtenir l'état du nom de service spécifié



Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Commandes de connectivité réseau

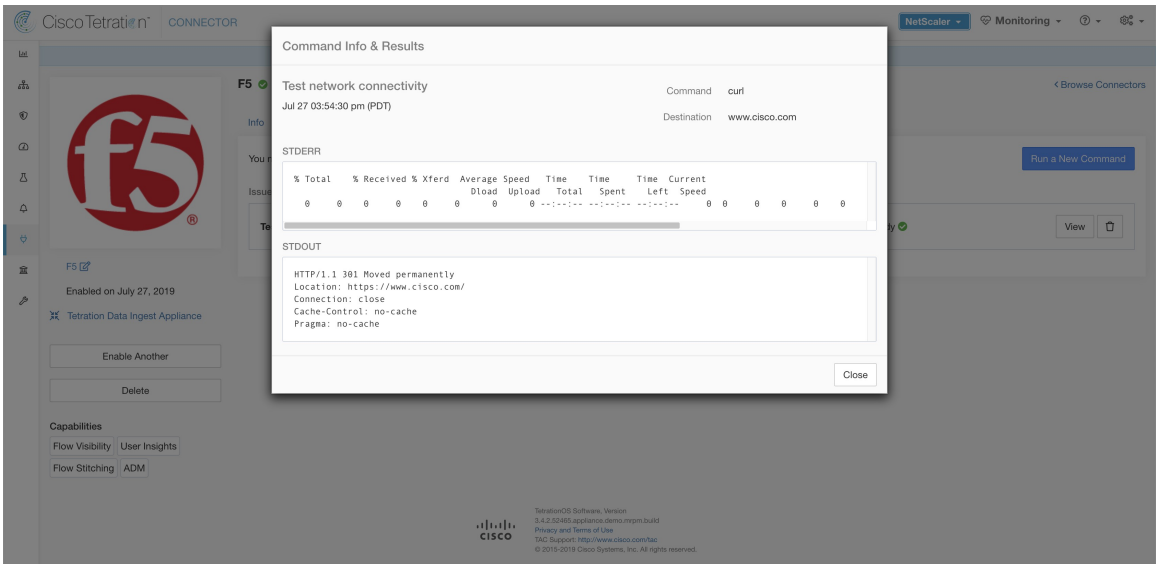
Tester la connectivité réseau à partir de l'appareil ou du connecteur. La commande est exécutée sur l'appareil par le contrôleur de l'appareil. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Commande réseau	liste déroulante	Commande de connectivité réseau à exécuter
	• *ping*	**ping -c 5 <destination>**
	• *boucle*	**curl -I <destination>**
Destination	chaîne	Destination à utiliser pour le test

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 96: Testez la connectivité réseau sur le connecteur F5 en exécutant une commande boucle



Répertorier les fichiers

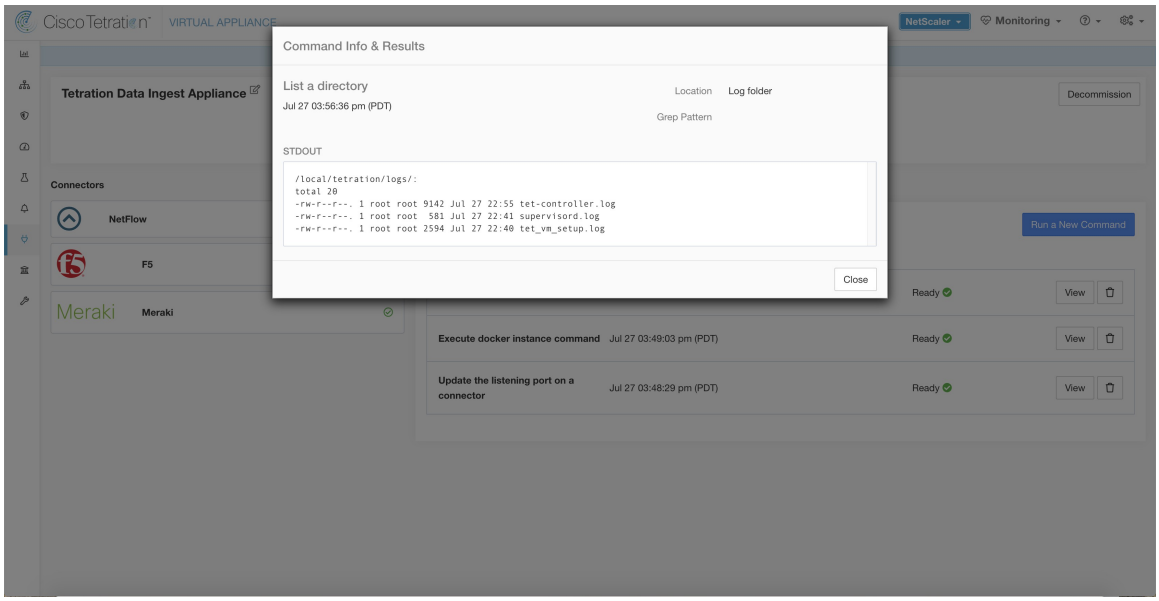
Répertoriez les fichiers dans les emplacements bien connus de l'appareil. Vous pouvez également utiliser la fonction grep pour un modèle spécifié. Cisco Secure Workload envoie la commande à l'appareil où la commande a été exécutée. Le contrôleur de l'appareil renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Site	liste déroulante	Répertorier les fichiers dans un emplacement cible
	• *Dossier de configuration du contrôleur*	Répertorie le contenu dans le dossier où sont conservés les fichiers de configuration du contrôleur.
	• *Dossier du certificat du contrôleur*	Répertorie le contenu dans le dossier où les certificats du contrôleur sont conservés.
	• *Dossier des journaux*	Répertorie le contenu dans le dossier où se trouvent les fichiers journaux.
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : aucun

Figure 97: Répertorier les fichiers du dossier journal de l'appareil d'acquisition Cisco Secure Workload



Répertorier les fichiers de service

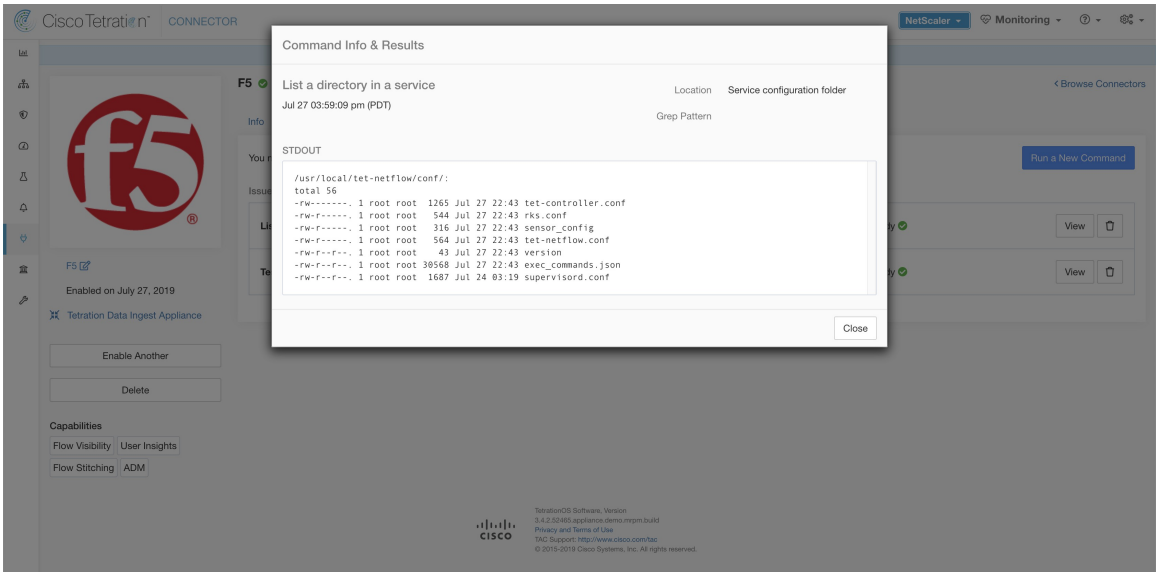
Répertoriez les fichiers dans les emplacements bien connus du service du connecteur. Vous pouvez également utiliser grep pour un modèle spécifié. Cisco Secure Workload envoie la commande au connecteur où la commande a été émise. Le contrôleur sur le service de connecteur renvoie le résultat. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Site	liste déroulante	Répertorier les fichiers dans un emplacement cible.
	• *Dossier de configuration du service*	Répertorie le contenu du dossier où les fichiers de configuration du service sont conservés.
	• *Dossier du certificat de service*	Répertorie le contenu du dossier où les certificats de service sont conservés.
	• *Dossier des journaux*	Répertorie le contenu dans le dossier où se trouvent les fichiers journaux.
	• *Dossier de base de données*	Répertorie le contenu du dossier où l'état des terminaux (en particulier pour les connecteurs AnyConnect et ISE) est conservé.
Modèle Grep	chaîne	Chaîne de modèles à extraire (grep) de la sortie

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 98: Répertorie les fichiers du dossier de configuration du connecteur F5 dans l'appareil d'acquisition Cisco Secure Workload



Capture de paquets

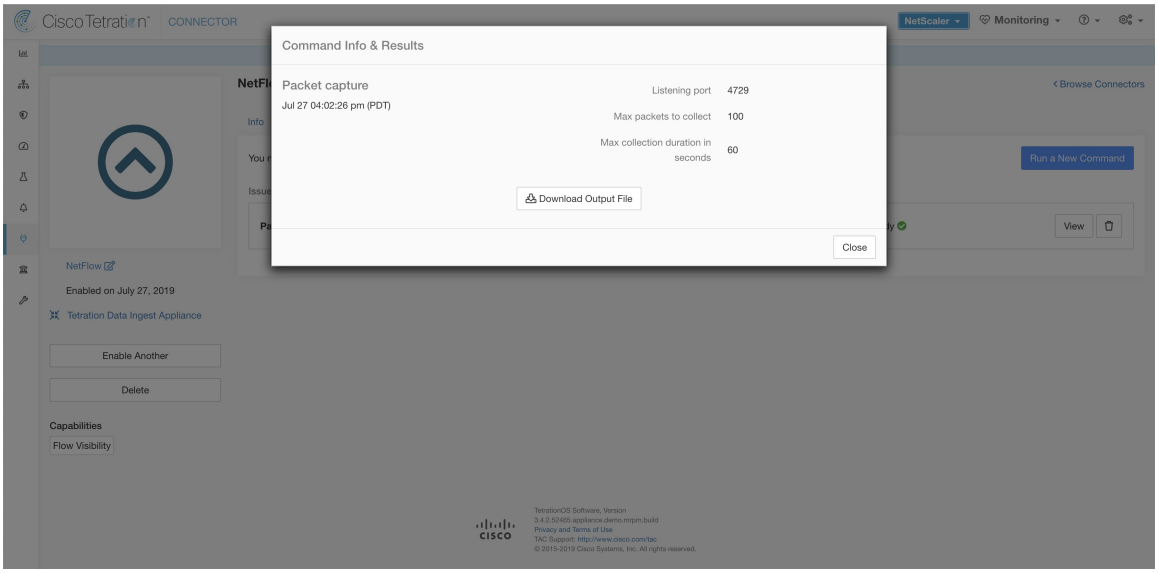
Capturer les paquets entrants sur un appareil ou un connecteur. Cisco Secure Workload envoie la commande à l'appareil/au connecteur où la commande a été exécutée. Le contrôleur du service de l'appareil ou du connecteur capture les paquets, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.pcap`.

Nom de l'argument	Type	Description
Port d'écoute	number	Capturer les paquets envoyés ou reçus sur ce port
Nombre maximal de paquets à collecter	number	Nombre maximal de paquets à collecter avant de renvoyer le résultat. Il doit être inférieur à 1000
Durée maximale de la collecte en secondes	number	Durée maximale à collecter avant de renvoyer le résultat. Elle doit être inférieure à 600 secondes.

Appliances virtuelles Cisco Secure Workload autorisées : toutes

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA et Meraki.

Figure 99: Capturer des paquets sur un port donné du connecteur NetFlow



Mettre à jour les ports d'écoute des connecteurs

Mettez à jour le port d'écoute sur un connecteur dans le dispositif d'acquisition Cisco Secure Workload. Cisco Secure Workload envoie la commande au contrôleur de l'appareil sur l'appareil sur lequel la commande est exécutée. Le contrôleur effectue les actions suivantes :

- Arrête le service Docker correspondant au connecteur.
- Recueille la configuration d'exécution actuelle du service.
- Supprime le service Docker.
- Met à jour la configuration d'exécution du service pour utiliser les nouveaux ports.
- Démarre un nouveau conteneur à partir de la même image Docker que celle utilisée dans le conteneur supprimé, avec de nouveaux ports accessibles. De plus, si un volume Docker a été monté sur le conteneur supprimé précédemment, le même volume est monté sur le nouveau conteneur.
- Renvoie les nouvelles liaisons IP du connecteur à Cisco Secure Workload.
- Cisco Secure Workload affiche le résultat dans une zone de texte.

Nom de l'argument	Type	Description
ID du connecteur	chaîne	ID de connecteur du connecteur pour lequel les ports d'écoute doivent être mis à jour
Étiquette de port d'écoute	liste déroulante	Le type de port qui est mis à jour.
	NET-FLOW9	Port d'écoute NetFlow v9
	IPFIX	Port d'écoute IPFIX

Nom de l'argument	Type	Description
Port d'écoute	chaîne	Nouveau port pour le connecteur

Appliances virtuelles Secure Workload autorisées : acquisition Cisco Secure Workload

Connecteurs autorisés : aucun

Figure 100: Mettre à jour le port d'écoute sur le connecteur Meraki à 2055 dans l'appareil d'acquisition Cisco Secure Workload

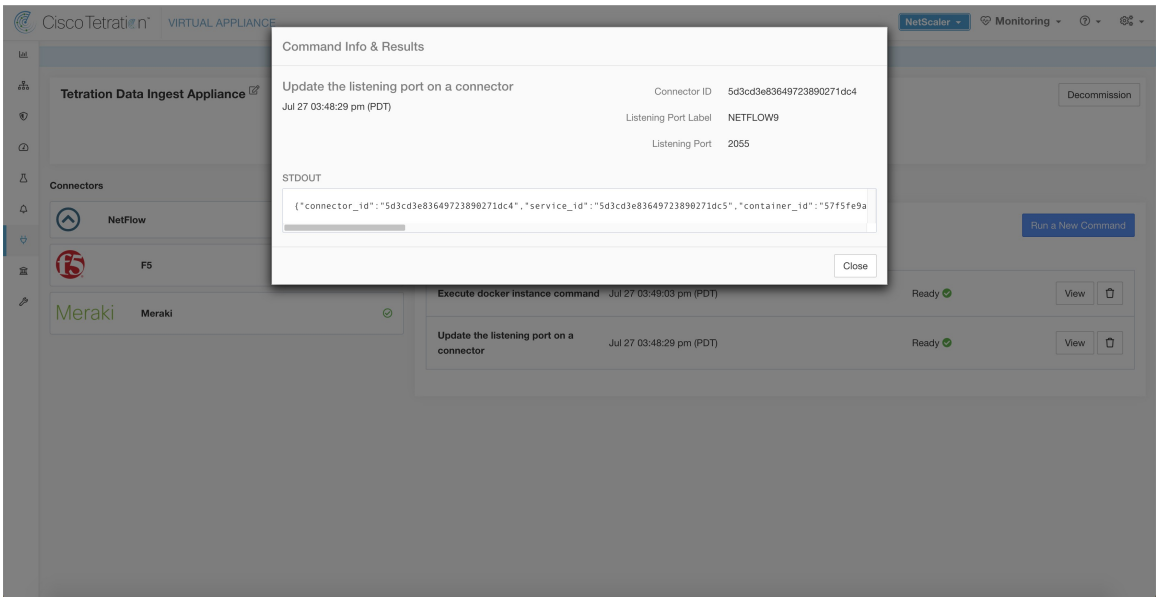
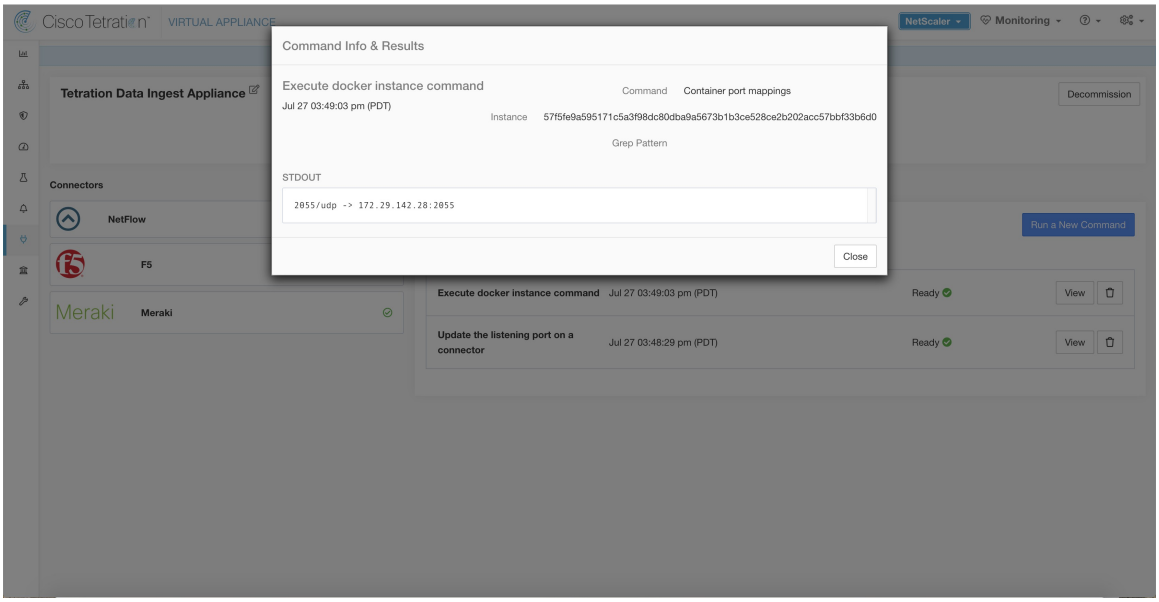


Figure 101: Récupérer les mappages de ports sur le connecteur Meraki dans l'appareil d'acquisition Cisco Secure Workload



Mettre à jour la configuration des journaux du connecteur de l'outil de notification d'alerte

Mettez à jour la configuration du journal pour le service Alert Notifier (TAN) de Cisco Secure Workloadqui héberge les connecteurs de notification d'alerte Syslog, de courriel, Slack, PagerDuty et Kinesis. Puisque le TAN héberge plusieurs connecteurs, la configuration du journal ne peut pas être mise à jour directement à partir de la page du connecteur. Cette commande autorisée permet à l'utilisateur de mettre à jour la configuration du journal.

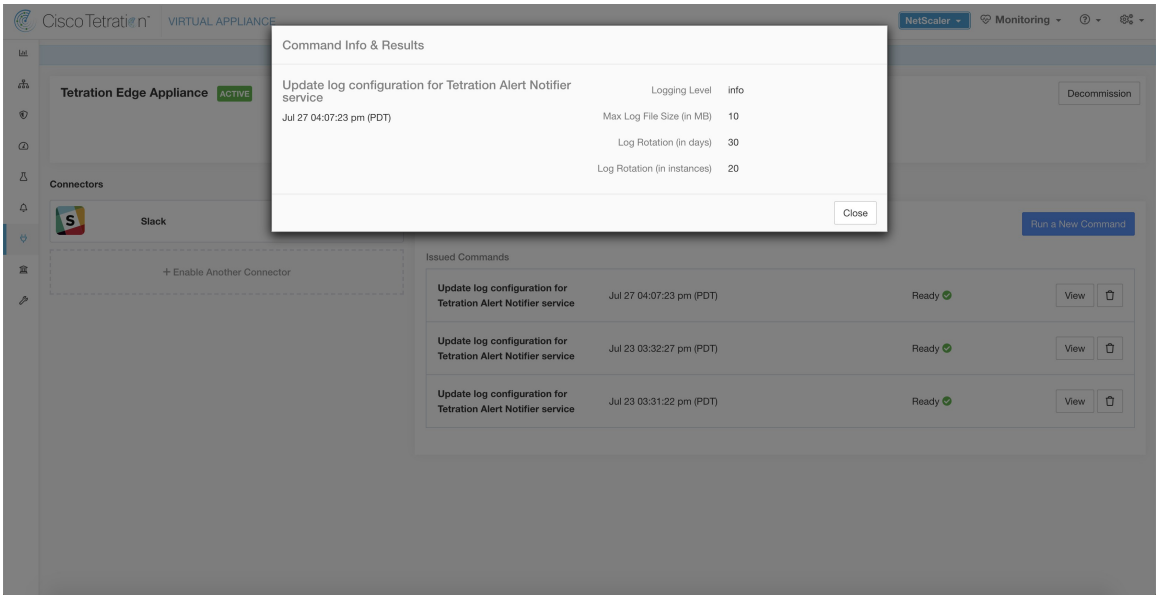
Cisco Secure Workload envoie la commande au contrôleur de service sur le service Docker TAN de l'appareil de périphérie Cisco Secure Workload. Le contrôleur applique la configuration au service et renvoie l'état de la mise à jour de la configuration.

Nom de l'argument	Type	Description
Niveau de journalisation	liste déroulante	Niveau de journalisation à utiliser par le service
	• *débogage*	Niveau de journal de débogage
	• *Information*	Niveau de journalisation informatif
	• *avertir*	Niveau du journal des avertissements
	• *erreur*	Niveau du journal des erreurs
Taille maximale du fichier journal (en Mo)	number	Taille maximale d'un fichier de journal avant le début de la rotation des journaux
Rotation des journaux (en jours)	number	Longévité maximale d'un fichier journal avant le début de la rotation des journaux
Rotation des journaux (dans les instances)	number	Nombre maximal d'instances de fichiers journaux conservées

Appliances virtuelles Cisco Secure Workload autorisées : Secure Workload Edge

Connecteurs autorisés :aucun

Figure 102: Mettre à jour la configuration des journaux sur le service Docker Alert Notifier Cisco Secure Workload dans l'appareil de périphérie Cisco Secure Workload.



Recueillir un instantané de l'appareil

Cisco Secure Workload envoie la commande à l'appareil où la commande a été exécutée. Lorsque le contrôleur de l'appareil reçoit cette commande de Cisco Secure Workload, il collecte les instantanés de l'appareil, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Fichiers inclus dans l'instantané :

- /local/tetration/appliance/appliance.conf
- /local/tetration/{logs, sqlite, user.cfg}
- /opt/tetration/tet_vm_setup/conf/tet-vm-setup.conf
- /opt/tetration/tet_vm_setup/docker/Dockerfile
- /opt/tetration/ova/version
- /usr/local/tet-controller/conf
- /usr/local/tet-controller/cert/{topic.txt, kafkaBrokerIps.txt}
- /var/run/supervisord.pid
- /etc/resolv.conf

Sorties de commande incluses dans l'instantané :

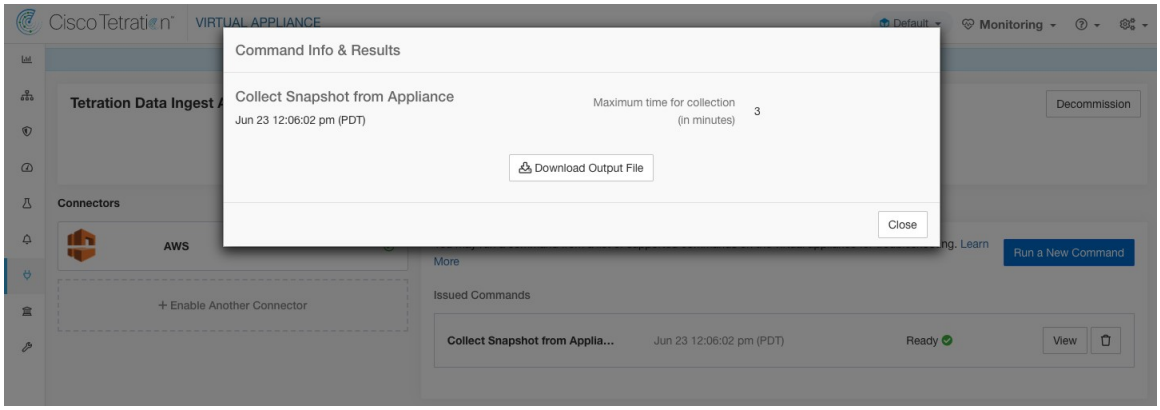
- ps aux
- iptables -L
- netstat {-nat, -rn, -suna, -stna, -tunlp}

- ss {-nat, -rn, -suna, -stna, -tunlp}
- /usr/local/tet-controller/tet-controller -version
- supervisorctl status
- rpm -qi tet-nic-driver tet-controller
- du -shc /local/tetration/logs
- ls {/usr/local/tet-controller/cert/, -l /local/tetration/sqlite/, -l /opt/tetration/tet_vm_setup/.tet_vm.done, -l/opt/tetration/tet_vm_setup/templates/}
- docker {images, ps -a}
- blkid/ifconfig/lscpu/uptime
- free -m
- df -h

Nom de l'argument	Type	Description
Durée maximale de la collecte en minutes	number	Durée maximale de la collecte avant l'envoi des résultats. Elle doit être inférieure à 20 minutes.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Figure 103: Recueillir un instantané de l'appareil Cisco Secure Workload



Recueillir l'instantané du connecteur

Cisco Secure Workload envoie la commande à l'appareil sur lequel le connecteur est déployé. Selon l'ID du connecteur, le contrôleur collecte les instantanés du connecteur, les code et renvoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format .tar.gz.

Fichiers inclus dans l'instantané :

- /usr/local/tet-netflow/conf

- /local/tetration/ {logs, SQLite}
- /var/run/ {supervisord.pid, tet-netflow.rid}

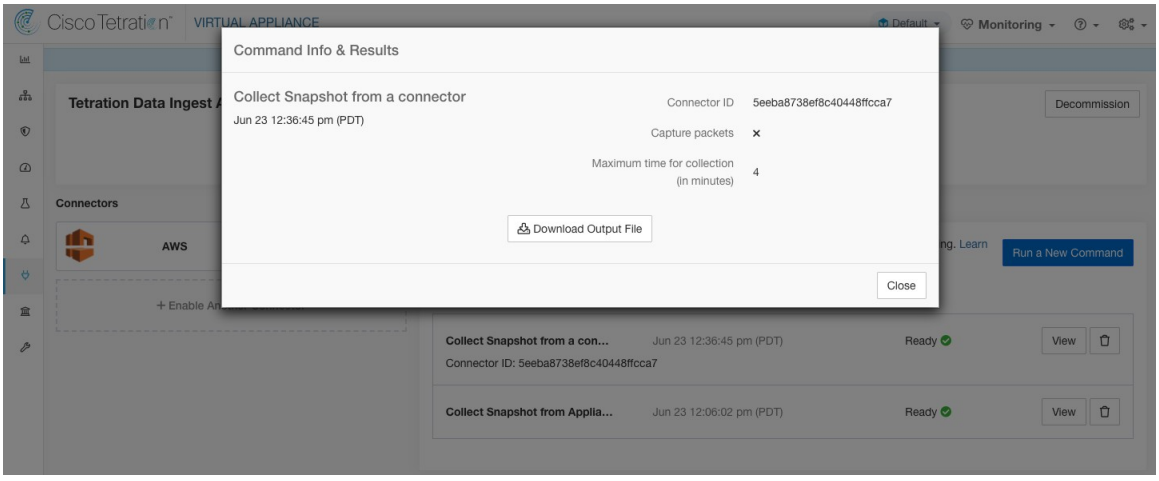
Sorties de commande incluses dans l'instantané :

- ps aux
- netstat {-nat, -rn, -suna, -stna, -tunlp}
- ss {-nat, -rn, -suna, -stna, -tunlp}

Nom de l'argument	Type	Description
ID du connecteur	chaîne	ID de connecteur du connecteur pour lequel la commande d'instantané est exécutée.
Capturer les paquets	case à cocher	Les paquets doivent-ils être capturés?
Max time for collection in minutes	number	Durée maximale de la collecte avant l'envoi des résultats. Elle doit être inférieure à 20 minutes.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Figure 104: Recueillir un instantané du connecteur Cisco Secure Workload sur l'ID de connecteur désigné



Recueillir le profil du contrôleur

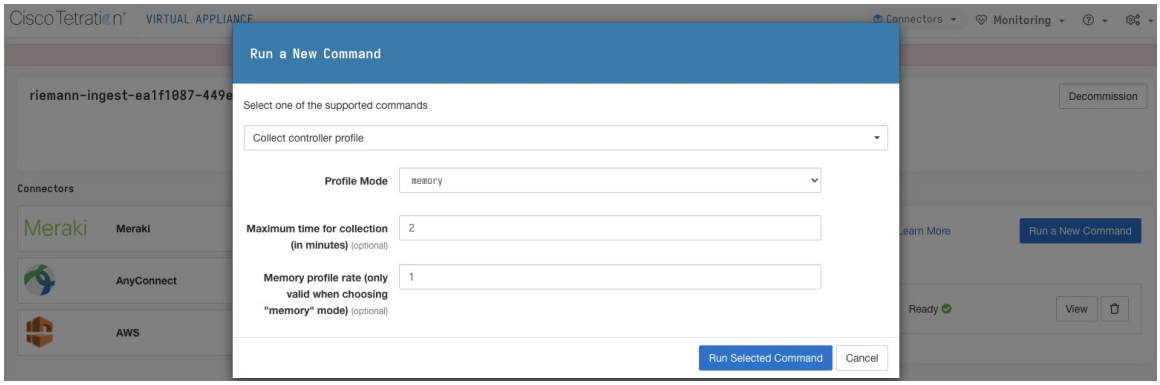
Recueillez les résultats du profilage de processus du contrôleur sur l'appareil ou les connecteurs. Cisco Secure Workload envoie la commande au connecteur où la commande a été exécutée. Le contrôleur de services redémarre le service de connecteur dans le mode de profilage spécifié. Après avoir obtenu le résultat de profilage, le contrôleur de service redémarre le service en mode normal et envoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Nom de l'argument	Type	Description
Profile Mode	liste déroulante	mode de profilage.
	• *memory*	Mode de profilage de mémoire.
	• *cpu*	mode de profilage du processeur (CPU).
	• *block*	Mode de profilage du bloc
	• *mutex*	Mode de profilage Mutex.
	• *goroutine*	Mode de profilage Goroutine.
Durée maximale de la collecte (en minutes)	number	Durée maximale de la collecte avant de renvoyer le résultat.
Débit du profil de mémoire (valide uniquement lorsque vous choisissez le mode « mémoire »)	number	Taux de profilage de mémoire. Ce champ est facultatif. S'il n'est pas fourni, la valeur par défaut dans Golan sera utilisée.

appliances virtuelles Cisco Secure Workload autorisées : acquisition Cisco Secure Workload et périphérie Cisco Secure Workload

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Email, Slack, PagerDuty, Kinesis, ISE, et Meraki.

Figure 105: Recueillir le profil du contrôleur de l'appareil Cisco Secure Workload



Recueillir le profil de connecteur

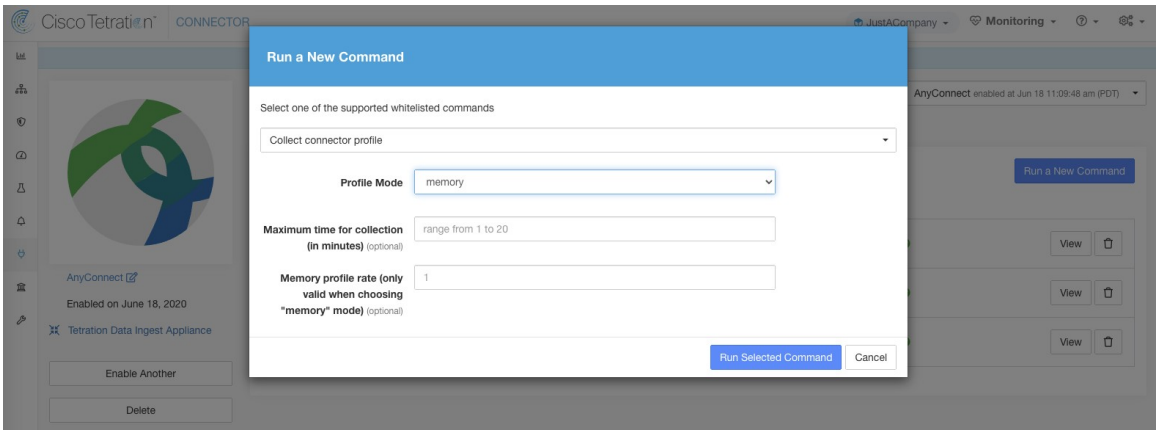
Recueillir les résultats du profilage des processus des connecteurs. Cisco Secure Workload envoie la commande au connecteur où la commande a été émise. Le contrôleur de services redémarre le service de connecteur dans le mode de profilage spécifié. Après avoir obtenu le résultat de profilage, le contrôleur de service redémarre le service en mode normal et envoie le résultat à Cisco Secure Workload. Lorsque les résultats sont disponibles chez Cisco Secure Workload, un bouton de téléchargement s'affiche pour télécharger le fichier au format `.tar.gz`.

Nom de l'argument	Type	Description
Profile Mode	liste déroulante	mode de profilage.
	• *memory*	Mode de profilage de mémoire.
	• *cpu*	mode de profilage du processeur (CPU).
	• *block*	Mode de profilage du bloc
	• *mutex*	Mode de profilage Mutex.
	• *goroutine*	Mode de profilage Goroutine.
Durée maximale de la collecte (en minutes)	number	Durée maximale de la collecte avant de renvoyer le résultat.
Débit du profil de mémoire (valide uniquement lorsque vous choisissez le mode « mémoire »)	number	Taux de profilage de mémoire. Ce champ est facultatif. S'il n'est pas fourni, la valeur par défaut dans Golan sera utilisée.

Appliances virtuelles Secure Workload autorisées : Cisco Secure Workload Ingest et Cisco Secure Workload Edge

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Email, Slack, PagerDuty, Kinesis, ISE, et Meraki.

Figure 106: Recueillir le profil de connecteur du connecteur Cisco Secure Workload



Remplacer l'intervalle d'alerte du connecteur pour l'appareil

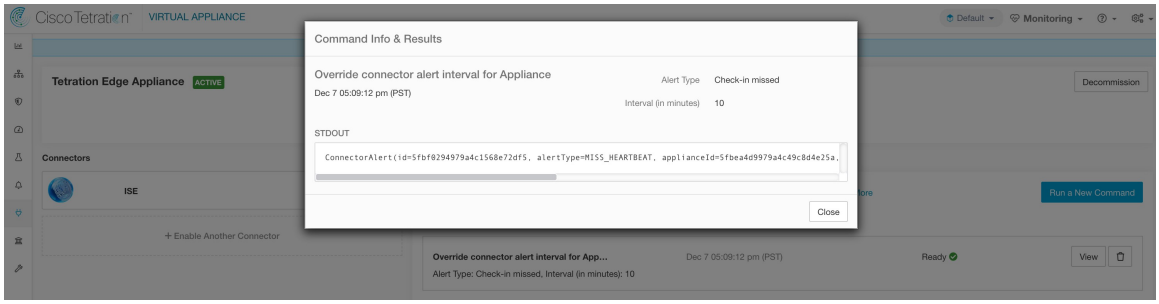
Remplacer l'intervalle d'alerte par défaut du connecteur de l'appareil. Cisco Secure Workload restreint l'envoi d'une seule alerte de connecteur par jour par défaut. Cette commande permet à l'administrateur de remplacer l'intervalle lorsqu'il estime qu'une fois par jour est trop long. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Type d'alerte	liste déroulante	Type d'alerte de connecteur à remplacer.
	• *Enregistrement manqué*	Vous avez manqué l'enregistrement de l'appareil.
	• *Utilisation du processeur*	Utilisation élevée
	• *Utilisation de la mémoire*	Utilisation élevée de la mémoire
	• *Utilisation du disque*	Utilisation élevée du disque.
Intervalle (en minutes)	number	Durée du remplacement de l'intervalle en minutes.

Appliances virtuelles Secure Workload autorisées : Cisco Secure Workload Ingest et Cisco Secure Workload Edge

Connecteurs autorisés : aucun

Figure 107: Remplacer l'intervalle d'alerte du connecteur pour l'appareil Cisco Secure Workload



Remplacer l'intervalle d'alerte du connecteur pour le connecteur

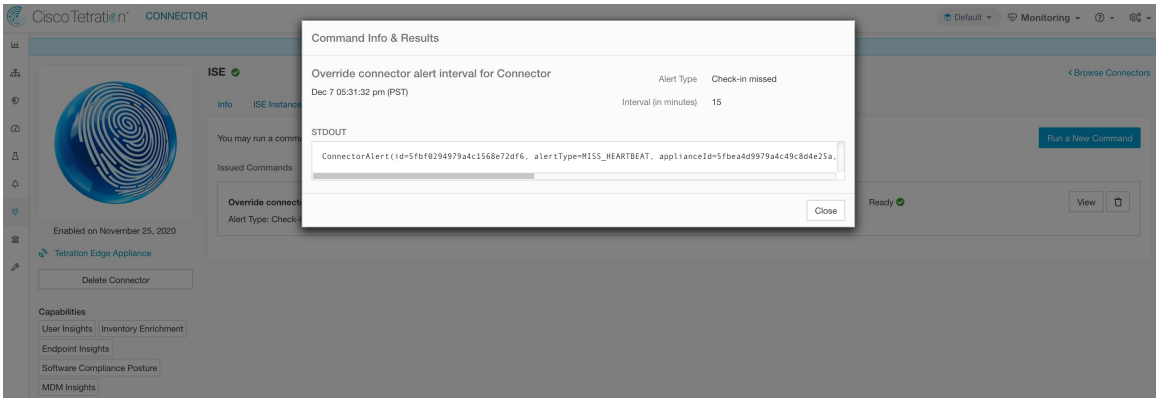
Remplacer l'intervalle d'alerte de connecteur par défaut pour le connecteur. Cisco Secure Workload restreint l'envoi à une seule alerte de connecteur par jour par défaut. Cette commande permet à l'administrateur de remplacer l'intervalle lorsqu'il estime qu'une fois par jour est trop long. Lorsque le résultat est disponible dans Cisco Secure Workload, il est affiché dans une zone de texte.

Nom de l'argument	Type	Description
Type d'alerte	liste déroulante	Type d'alerte de connecteur à remplacer.
	• *Enregistrement manqué*	Il manque l'enregistrement du connecteur.
Intervalle (en minutes)	number	Durée du remplacement de l'intervalle en minutes.

Appliances virtuelles Cisco Secure Workload autorisées : aucune

Connecteurs autorisés : NetFlow, NetScaler, F5, AnyConnect, Syslog, Courriel, Slack, PagerDuty, Kinesis, ISE, ASA, Meraki, ServiceNow, WAD.

Figure 108: Remplacer l'intervalle d'alerte du connecteur pour le connecteur Cisco Secure Workload



Tableaux de bord Hawkeye

Les tableaux de bord Hawkeye fournissent des informations sur l'intégrité des connecteurs et des appliances virtuelles lorsque les connecteurs sont activés.

Tableau de bord du contrôleur d'appareil

Le tableau de bord du contrôleur d'appareil fournit des informations sur les statistiques du réseau et les mesures du système telles que le pourcentage d'utilisation du processeur, de la mémoire, du disque et le nombre de descripteurs de fichiers ouverts.

Figure 109: Tableau de bord du contrôleur d'appareil

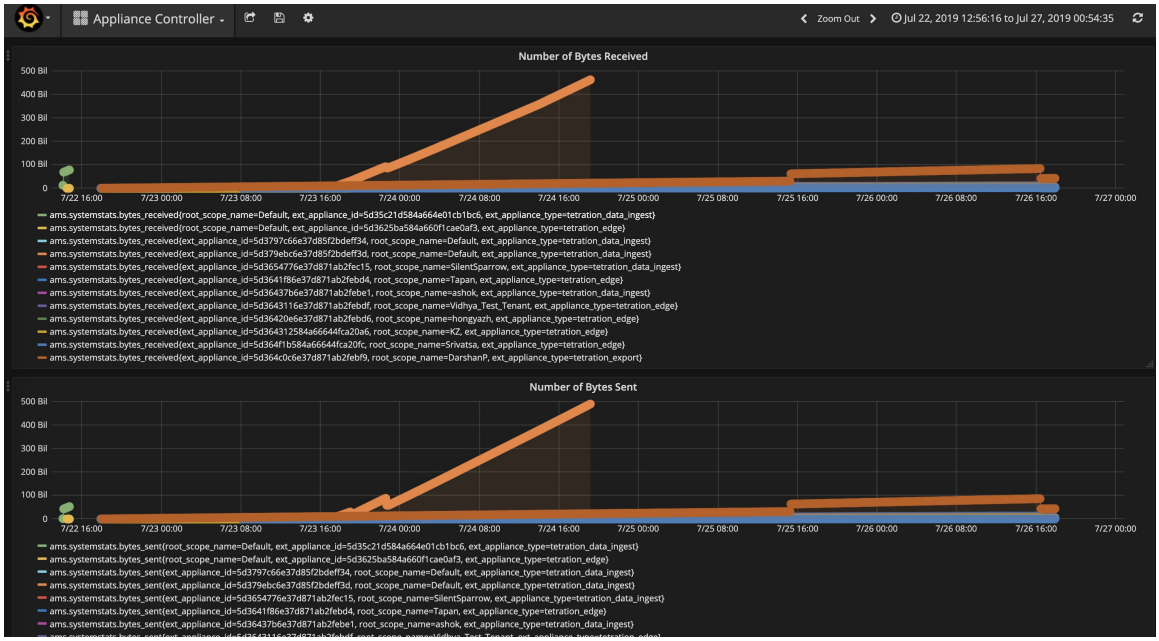


Tableau de bord du service

Le tableau de bord du service fournit des renseignements sur les mesures d'exportation, le cas échéant, y compris le nombre d'observations de flux exportées vers Cisco Secure Workload, le nombre de paquets exportés vers Cisco Secure Workload et le nombre d'octets exportés vers Cisco Secure Workload. En outre, ce tableau de bord fournit des informations sur le traitement et le décodage du protocole (par exemple, les services qui traitent NetFlow v9 et IPFIX). Des mesures telles que le nombre décodé, le nombre d'erreurs décodées, le nombre de flux, le nombre de paquets et le nombre d'octets sont disponibles dans ce tableau de bord. En outre, les mesures du système pour le conteneur Docker où le service est exécuté sont également incluses dans ce tableau de bord. Des mesures telles que le pourcentage d'utilisation du processeur, le pourcentage d'utilisation de la mémoire, le pourcentage d'utilisation du disque et le nombre de descripteurs de fichiers ouverts font partie de ce tableau de bord.

Figure 110: Tableau de bord du service

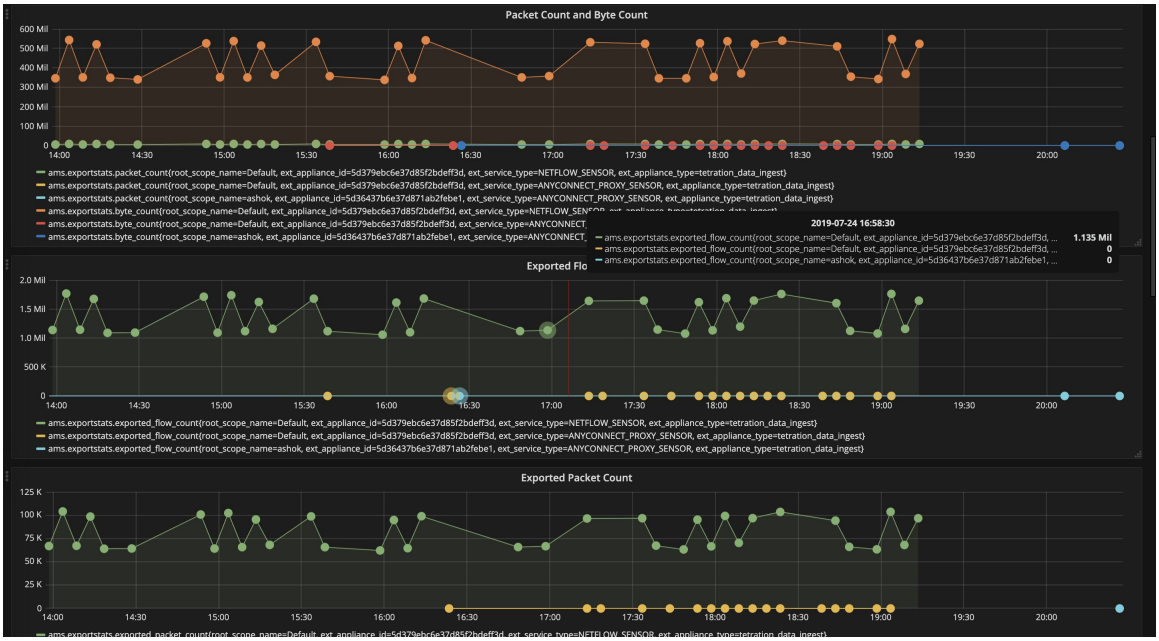


Tableau de bord du service AnyConnect

Le tableau de bord du service AnyConnect fournit des renseignements sur le service spécifique à AnyConnect. Les mesures telles que le nombre de points terminaux, le nombre d'inventaires et le nombre d'utilisateurs rapportés par le connecteur AnyConnect à Cisco Secure Workload sont disponibles dans ce tableau de bord. En outre, ce tableau de bord fournit également des renseignements sur le traitement et le décodage du protocole IPfix. Des mesures telles que le nombre décodé, le nombre d'erreurs décodées, le nombre de flux, le nombre de paquets et le nombre d'octets sont disponibles dans ce tableau de bord.

Figure 111: Tableau de bord AnyConnect

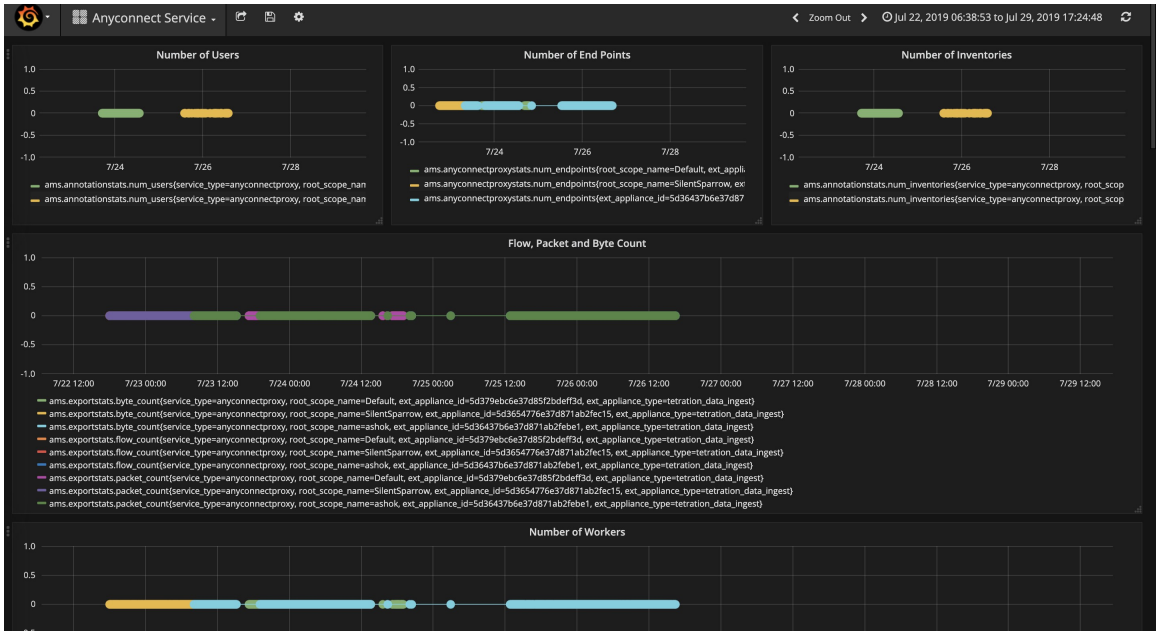
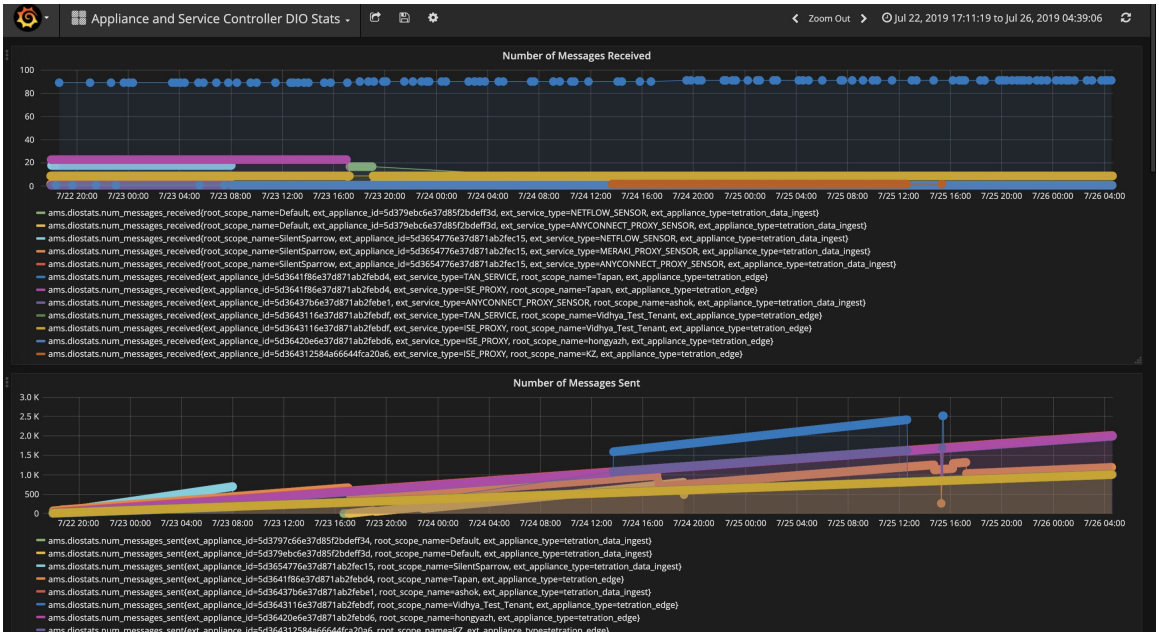


Tableau de bord de l'appareil et du service DIO

Le tableau de bord des appareils et des services DIO fournit des renseignements sur le nombre de messages échangés dans la rubrique Kafka sur laquelle communiquent le gestionnaire d'appareils et les contrôleurs des appareils et services. Des mesures telles que le nombre de messages reçus, le nombre de messages envoyés et le nombre de messages en échec sont incluses dans ce tableau de bord. En outre, le dernier décalage lu par les contrôleurs est également fourni pour comprendre si le contrôleur est en retard dans le traitement des messages de contrôle du gestionnaire.

Figure 112: Tableau de bord de l'appareil et du service DIO



Directives générales de dépannage

Une fois qu'un connecteur est affiché à l'état actif dans la page des connecteurs de Cisco Secure Workload, aucune action n'est nécessaire sur l'appareil sur lequel le connecteur est activé; l'utilisateur n'a pas besoin de s'y connecter. Si ce n'est pas le cas, les renseignements suivants vous aideront à résoudre ces problèmes.

Dans des conditions normales, sur l'appareil :

- `systemctl status tet_vm_setup.service` signale un service *inactif* avec l'état de sortie *SUCCESS*.
- `systemctl status tet-nic-driver` signale un service *actif* .
- `supervisorctl status tet-controller` signale un service *RUNNING (EN COURS D'EXÉCUTION)* . Cela indique que le contrôleur de l'appareil est opérationnel.
- `docker network ls` signale trois réseaux : `pont`, `hôte` et `aucun`.
- `docker ps` signale les conteneurs en cours d'exécution sur l'appareil. En règle générale, lorsqu'un connecteur est activé avec succès sur un appareil, un conteneur Docker est instancié sur l'appareil. Pour les connecteurs Syslog, Courriel, Slack, PagerDuty et Kinesis, un service de notification d'alertes Cisco Secure Workload est instancié en tant que conteneur Docker sur l'appareil de périphérie Cisco Secure Workload.
- `docker logs <cid>` pour chaque conteneur doit signaler que tet-netflowensor est entré à l'état RUNNING.
- `docker exec <cid> ifconfig` ne signale qu'une seule interface, en plus de la boucle avec retour;
- `docker exec <cid> netstat -rn` signale la passerelle par défaut.
- `cat /local/tetration/appliance/appliance.conf` sur l'appareil pour voir la liste des services Docker en cours d'exécution sur celui-ci. Il comprend des détails sur l'ID de service, l'ID du connecteur, le conteneur, l'ID d'image et les mappages de port (le cas échéant). Sur un appareil d'acquisition Cisco

Secure Workload, trois services au maximum doivent être exécutés sur l'appareil. Les mappages de ports et les volumes Docker montés sur les conteneurs sont disponibles dans ce fichier.

Figure 113: Service et état de déploiement d'appareils Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# systemctl status tet_vm_setup.service
● tet_vm_setup.service - Tetration Appliance Setup
   Loaded: loaded (/etc/systemd/system/tet_vm_setup.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Sat 2019-07-27 23:51:29 UTC; 21h ago
 Main PID: 1249 (code=exited, status=0/SUCCESS)

Jul 27 23:51:12 localhost.localdomain python[1249]: mount: /dev/sr0 is write-protected, mounting read-only
Jul 27 23:51:29 esx-2106-ingest python[1249]: Docker version 18.09.8, build 0dd43dd87f
Jul 27 23:51:29 esx-2106-ingest python[1249]: REPOSITORY          TAG                 IMAGE ID            CREATE... SIZE
Jul 27 23:51:29 esx-2106-ingest python[1249]: userPrivateKey.key
Jul 27 23:51:29 esx-2106-ingest python[1249]: intermediateCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaBrokerIps.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: userCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: topic.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: Created symlink from /etc/systemd/system/multi-user.target.wants/s...vice.
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 114: État du service de pilote réseau Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# systemctl status tet-nic-driver.service
● tet-nic-driver.service - NIC network driver plugin for Docker
   Loaded: loaded (/etc/systemd/system/tet-nic-driver.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2019-07-27 23:51:12 UTC; 21h ago
 Main PID: 733 (nic)
   Memory: 4.4M
   CGroup: /system.slice/tet-nic-driver.service
           └─733 /usr/local/tet/nic-driver/nic -log-level debug

Jul 27 23:51:12 localhost.localdomain systemd[1]: Started NIC network driver plugin for Docker.
Jul 27 23:51:12 localhost.localdomain systemd[1]: Starting NIC network driver plugin for Docker...
Jul 27 23:51:12 localhost.localdomain nic[733]: time="2019-07-27T23:51:12Z" level=info msg="NIC network driver started"
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 115: État du contrôleur de l'appareil

```
[root@esx-2106-ingest tetter]# supervisorctl status tet-controller
tet-controller                   RUNNING   pid 1971, uptime 21:43:29
[root@esx-2106-ingest tetter]#
```

Si l'une des situations précédentes n'est pas vérifiée, vérifiez les journaux du script de déploiement dans /local/tetration/logs pour connaître la raison de l'échec du déploiement de l'appareil et/ou du connecteur.

Vous pouvez résoudre tout autre problème d'enregistrement ou de connectivité du connecteur comme suit.

`docker exec <cid> ps -ef` signale les instances tet-netflowsensor-engine, `/usr/local/tet/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf`, ainsi que l'instance de gestionnaire de processus `/usr/bin/supervisord -c /usr/local/tet-netflow/ conf/supervisord.conf -n`.

Figure 116: Exécution des processus sur le connecteur ASA de Cisco Secure Firewall dans le dispositif d'acquisition Cisco Secure Workload

```
[root@esx-2106-ingest tetter]# docker ps
CONTAINER ID        IMAGE                                                                                COMMAND
     CREATED             STATUS              PORTS                                NAMES
c82decfaa877        asa_sensor-3.4.2.52465.appliance.demo.mrpm.build-asa:5d3ce5e43649723890271dd3   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours         172.29.142.27:4729->4729/udp   asa-5d3ce5e43649723890271dd3
eddd5cd59839        aws_sensor-3.4.2.52465.appliance.demo.mrpm.build-aws:5d3ce3b73649723890271dce   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours                                      aws-5d3ce3b73649723890271dce
[root@esx-2106-ingest tetter]# docker exec c8 ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 00:01 ?        00:00:15 /usr/bin/python /usr/bin/supervisord -c /usr/local/tet-netflow/conf/supe
rvisord.conf -n
root         8     1  0 00:01 ?        00:02:24 /usr/local/tet-netflow/tet-netflowsensor-engine -ctrl-config /usr/local/
tet-netflow/conf/tet-controller.conf -upgrade-script /usr/local/tet-netflow/scripts/check_config_update.sh -service /usr
/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf
root     27002     8  0 21:31 ?        00:00:00 /usr/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/
conf/tet-netflow.conf
root     27024     0  0 21:32 ?        00:00:00 ps -ef
[root@esx-2106-ingest tetter]#
```

Journaliser les fichiers

Les commandes suivantes peuvent être utilisées pour afficher les journaux de divers services sur l'appareil.

- **/local/tetration/logs/tet-controller.log** affiche les journaux du contrôleur d'appareil.
- **docker exec <cid> cat /local/tetration/logs/tet-controller.log** affiche les journaux du contrôleur de service sur le connecteur.
- **exécutable Docker** <cid> cat /local/tetration/logs/tet-netflow.log affiche les journaux du service de connecteur.
- **docker exec <cid> cat /local/tetration/logs/tet-ldap-loader.log** affiche les journaux de création d'instantané LDAP (si la configuration LDAP est applicable au connecteur).
- **docker exec <cid> cat /local/tetration/logs/check_conf_update.log** affiche les journaux d'interrogation de la mise à jour de la configuration (pour les connecteurs sur l'appareil d'acquisition).

Note Il existe un ensemble autorisé de commandes sur Cisco Secure Workload qui peuvent extraire ces journaux de l'appareil et/ou des connecteurs directement. Pour en savoir plus, consultez Ensemble de commandes autorisé.

Mode de débogage

Le niveau de journalisation par défaut pour l'appareil/le contrôleur de service et le service de connecteur est défini au niveau *info*. Pour résoudre les problèmes, il se peut que nous devions définir l'agent en mode *débogage*. Pour ce faire, mettez à jour la configuration du journal sur l'appareil/le connecteur sur Cisco Secure Workload directement pour l'appareil ou le connecteur souhaité. Les niveaux de journalisation du contrôleur et des services sont mis à jour si la configuration est mise à jour sur le connecteur. Pour en savoir plus, consultez Configuration de la journalisation (Configuration des journaux).

Cisco Secure Firewall Management Center

Combine the power of Cisco Secure Workload with the power of Cisco's Secure Firewall (formerly known as Cisco Firepower) for a security solution that makes use of:

- Segmentation

  Firewall-based segmentation is suitable for workloads where software agents are not installed. However, you can also use this method for agent-based workloads. You can easily and broadly apply different sets of policies for traffic entering your network, for traffic exiting your network, and for traffic between workloads within your network.

- Virtual Patching

  Virtual patching adds Intrusion Prevention System (IPS) protection to workloads where software agents are installed. Use this integration to avoid malicious traffic entering the application. With the Virtual Patching Config, Secure Workload publishes the CVEs to the FMC to consider while creating the IPS policies.

With this integration, Secure Workload automatically enforces and manages segmentation policies on the Secure Firewall Threat Defense (formerly known as Firepower Threat Defense) firewalls managed by the Secure Firewall Management Center instance. Policies are updated dynamically, and the set of workloads to which policies apply is refreshed continually as the application environment changes.

Network inventory is dynamically updated by the Secure Workload inventory filters on which your segmentation policies are based; when workloads are added, changed, or removed from your network, Secure Workload automatically updates the Dynamic Objects in Secure Firewall Management Center on which the corresponding access control rules are based. All enforced policy changes are automatically deployed to managed Secure Firewall Threat Defense (formerly known as Firepower Threat Defense or FTD) devices; you never need to redeploy changes in Secure Firewall Management Center.

For complete information about this integration, including more details about how it works, supported platforms, limitations, setup instructions for both products, and troubleshooting information, see the Cisco Secure Workload and Cisco Secure Firewall Management Center Integration Guide.

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.