Orchestrateurs externes dans Cisco Secure Workload

Les orchestrateurs externes sont utilisés pour rassembler les métadonnées existantes décrivant vos charges de travail à partir des systèmes de votre réseau. Certains orchestrateurs externes peuvent également appliquer la politique de segmentation.

Pour les déploiements pour lesquels un système d'enregistrement autorisé avec des étiquettes pour les charges de travail existe, nous offrons un moyen d'importer automatiquement les étiquettes au moyen d'intégrations d'orchestrateurs externes. Toute modification dans le système d'enregistrement sera apprise automatiquement par Cisco Secure Workload et utilisée pour la mise à jour des étiquettes de votre inventaire.

Pour des renseignements détaillés sur la puissance et les utilisations des étiquettes, consultez Étiquettes de charge de travail.

En raison des récentes mises à jour de l'interface graphique, certaines images ou captures d'écran utilisées dans le guide de l'utilisateur peuvent ne pas refléter pleinement la conception actuelle du produit. Nous recommandons d'utiliser ce guide en conjonction avec la dernière version du logiciel pour obtenir la référence visuelle la plus précise.

Accéder à la page des orchestrateurs externes

La page principale pour les orchestrateurs externes est accessible en sélectionnant **Manage (Gestion)** > **Workloads(Charges de travail)** > **External Orchestrators (Orchestrateurs externes)** dans la barre de menus à gauche.

Liste des orchestrateurs externes

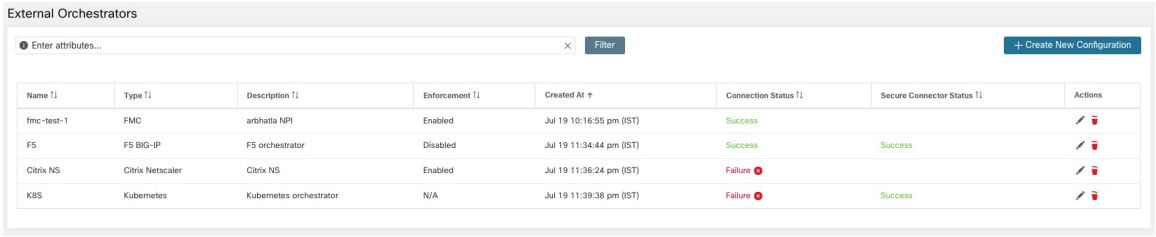
La page External Orchestrateurs (Orchestrateurs externes) affiche les orchestrateurs externes existants et fournit des fonctions pour les modifier et les supprimer ainsi que pour en créer de nouveaux :

Table 1: Orchestrateurs externes

Type	Description/Quand l'utiliser
VMware vCenter	Pour importer les données de la machine virtuelle, tels que le nom d'hôte, l'adresse IP et les étiquettes, d'un serveur vCenter vers Cisco Secure Workload. Les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.
Amazon Web Services	(Vous ne pouvez pas créer de nouveaux orchestrateurs AWS; créez plutôt des connecteurs AWS. Consultez la section Connecteur AWS. Tous les orchestrateurs AWS existants sont en lecture seule). Pour importer les données des instances de serveur EC2, telles que le nom d'hôte, l'adresse IP et les étiquettes, depuis le compte AWS vers Cisco Secure Workload. Les étiquettes générées sont utiles pour créer des portées et des politiques Cisco Secure Workload.
Kubernetes/OpenShift	Pour importer les entités de Kubernetes, telles que les nœuds, les pods, les services et les étiquettes. Ces étiquettes peuvent être utilisées au sein de Cisco Secure Workload pour définir des portées et des politiques.
DNS	Pour importer des enregistrements A/AAAA et CNAME à partir d'un serveur DNS par transfert de zone. Cela produit des noms DNS sous forme d'étiquettes, qui sont utiles pour définir les portées et les politiques Cisco Secure Workload.

Type	Description/Quand l'utiliser
Infoblox	Pour importer des réseaux, des hôtes et des enregistrements A/AAAA avec des attributs extensibles à partir d'un appareil Infoblox avec IPAM/DNS activé. Les attributs extensibles importés peuvent être utilisés comme étiquettes dans les portées et les politiques Cisco Secure Workload.
F5 BIG-IP	Pour lire les configurations de serveur virtuel à partir d'un équilibreur de charge F5 donné et générer des étiquettes pour les services fournis, qui peuvent être utilisés pour définir les politiques d'application dans Cisco Secure Workload. La fonction d'application de la politique les traduira en règles F5 à l'aide de l'API REST F5.
Citrix Netscaler	Pour lire les configurations de serveur virtuel à partir d'un équilibreur de charge Netscaler donné et générer des étiquettes pour les services fournis, qui peuvent être utilisés pour définir des politiques d'application dans Cisco Secure Workload. La fonctionnalité d'application des politiques les traduira en ACL Netscaler via son API REST.
Cisco Secure Firewall Management Center	Pour déployer les politiques sur tous les périphériques Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense ou FTD) enregistrés sur Cisco Secure Firewall Management Center à l'aide de l'API REST.

Figure 1: Orchestrateur externe

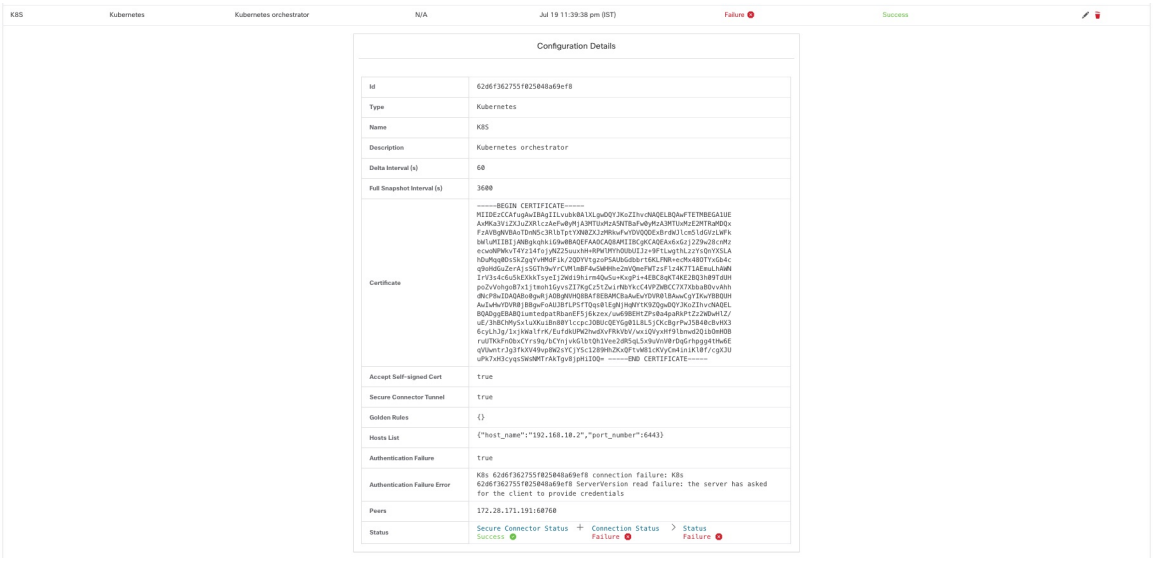


Chaque ligne affiche une version abrégée de l'orchestrateur externe comportant son *nom*, son *type*, sa *description*, son *application*, son statut *Créé à*, l'état de *la connexion* et l'*état du connecteur sécurisé Secure Connector*. L'état de la connexion indique si une connexion à une source de données externe a pu être établie avec succès. *Secure Connector Status* (État du connecteur sécurisé) affiche l'état du tunnel Secure Connector (succès ou échec). Si le tunnel n'est pas activé, N/A s'affiche.

Activez le tunnel du connecteur sécurisé lors de la création d'une configuration d'orchestrateur externe. Si le tunnel de connecteur sécurisé est activé, « l'état de la connexion » de l'orchestrateur externe dépend à la fois de l'état d'authentification et de l'état du connecteur sécurisé. Si le tunnel du connecteur sécurisé n'est pas activé, « l'état de la connexion » de l'orchestrateur externe dépend uniquement de l'état d'authentification. Quel que soit l'état (réussite ou échec), vous pouvez cliquer sur la ligne respective pour obtenir plus de détails.

Pour plus de détails sur les mesures du client du connecteur sécurisé, cliquez sur la ligne **Status** (État) ou, dans le volet gauche, accédez à **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (connecteur sécurisé)**.

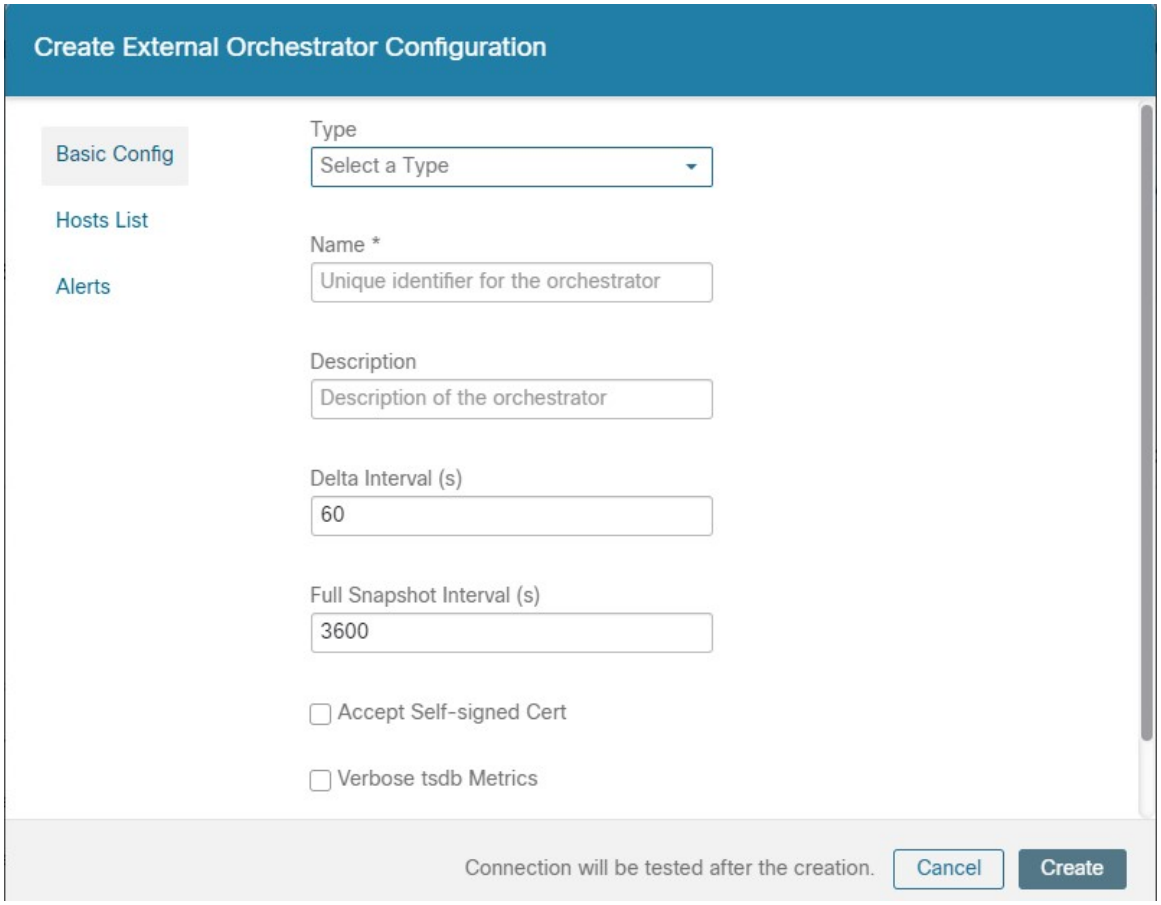
Figure 2: Échec de l'authentification de l'orchestrateur externe



Créer un orchestrateur externe

Un orchestrateur externe peut être créé en cliquant sur le bouton **Create New Configuration** (Créer une nouvelle configuration) dans la page principale des orchestrateurs externes. Une boîte de dialogue modale s'ouvre, dans laquelle vous pouvez saisir un nom et choisir un type d'orchestrateur externe. L’image ci-dessous montre la page de configuration de base :

Figure 3: Créer une configuration d'orchestrateur externe



Le tableau suivant décrit les champs communs aux orchestrateurs externes. Selon le type sélectionné, la page de *configuration de base* nécessite la saisie de paramètres supplémentaires. Ceux-ci seront couverts par la section respective des orchestrateurs externes individuels ci-dessous.

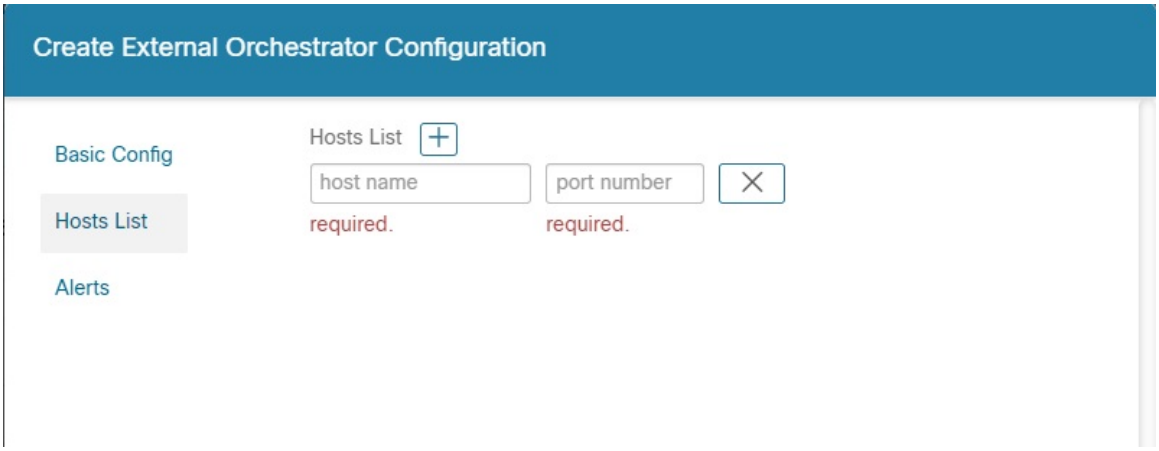
Champs communs	Obligatoire	Description
Type	Oui	Sélectionnez un orchestrateur externe dans la liste.
Nom	Oui	Nom de l'orchestrateur externe, qui doit être unique pour le détenteur actif.
Description	Non	Description de l'orchestrateur externe.
Intervalle(s) complet(s) de l'instantané	Oui	Intervalle en secondes pendant lequel l'orchestrateur externe tentera d'importer l'instantané complet de la configuration à partir du *Type* sélectionné.

Champs communs	Obligatoire	Description
Accept Self-signed Cert (Accepter le certificat autosigné)	Non	Cochez cette option pour accepter les certificats de serveur autosignés pour la connexion HTTPS utilisée par Cisco Secure Workload afin de récupérer les données de configuration du *Type*. Par défaut, les certificats de serveur autosignés ne sont pas autorisés.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Non	Cochez cette option pour définir les connexions à la grappe Cisco Secure Workload pour qu'elles soient acheminées par un tunnel de connecteur sécurisé.

Note Les champs *Intervalle différentiel* et *Mesures TSDB détaillées*, comme le montre l'image ci-dessus sont facultatifs et applicables uniquement à certains orchestrateurs externes, qui sont présentés dans les descriptions respectives ci-dessous.

À l'exception du type d'orchestrateur externe *AWS*, la *Hosts List* (Liste des hôtes) doit être fournie. Elle spécifie les adresses réseau de la source de données externe à partir de laquelle l'orchestrateur externe récupérera les données et générera des étiquettes. Pour ce faire, cliquez sur l'onglet *Hosts List* (liste des hôtes) sur le côté gauche, comme le montre l'image suivante :

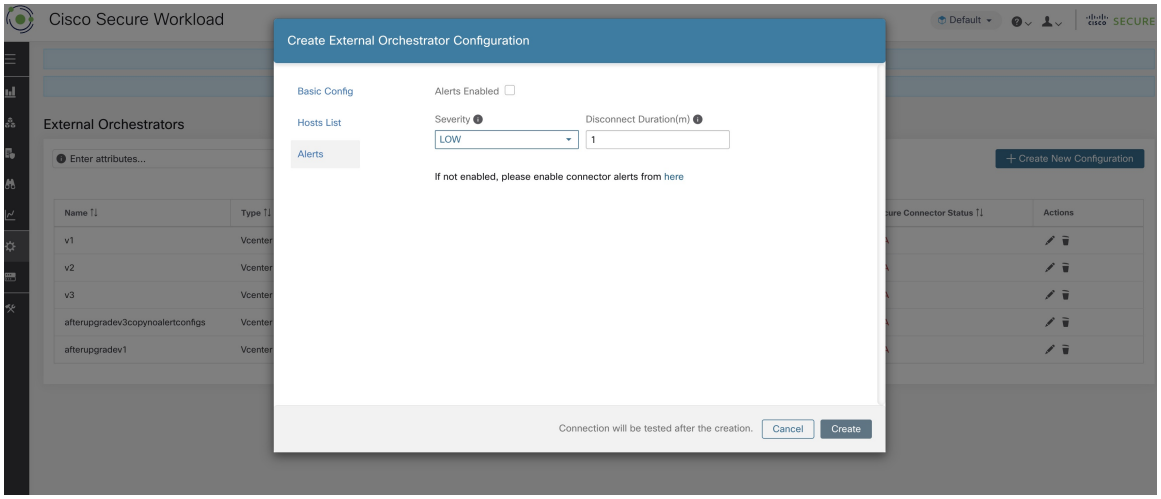
Figure 4: Liste des hôtes de l'orchestrateur externe



Pour ajouter une nouvelle entrée à la liste d'hôtes, cliquez sur le signe +. Chaque ligne doit contenir un nom d'hôte DNS valide, une adresse IPv4 ou IPv6 et un numéro de port. Selon le type d'orchestrateur externe choisi, vous pouvez saisir plusieurs hôtes à des fins de haute disponibilité ou de redondance. Pour en savoir plus, consultez la description de l'orchestrateur externe choisi.

Pour définir l'alerte pour l'orchestrateur externe, vous pouvez le faire en cliquant sur l'onglet *Alerte* sur le côté gauche, comme le montre l'image suivante :

Figure 5: Alertes de l'orchestrateur externe



Pour chaque orchestrateur externe, la configuration des *alertes* nécessite que des paramètres supplémentaires soient fournis. Ceux-ci seront couverts par la section respective des orchestrateurs externes individuels ci-dessous.

Pour activer les alertes pour cet orchestrateur externe, cochez la case *Alert Enabled* (alerte activée).

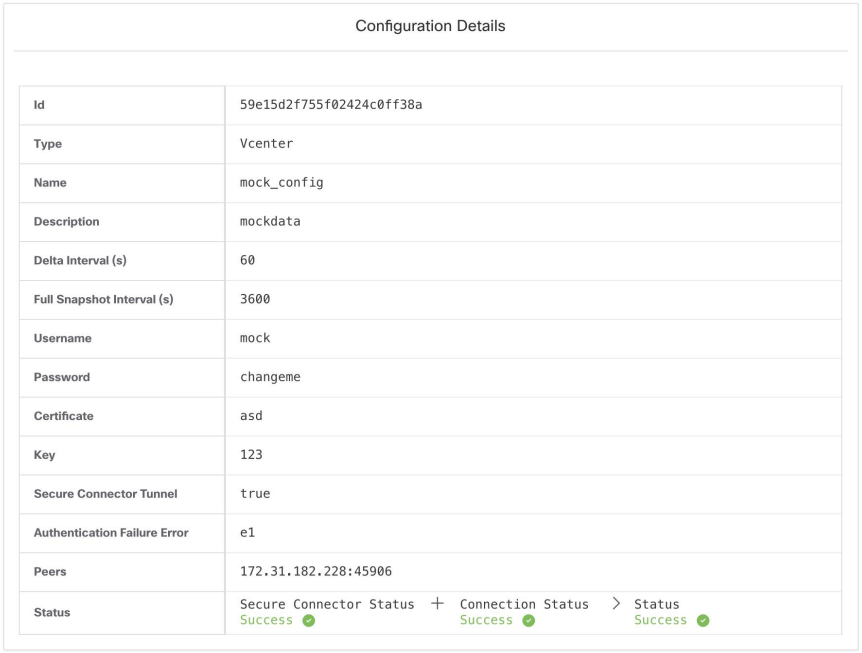
Note Assurez-vous que les alertes du connecteur sont également activées sur la page **Manage** > **Workloads** > **Alert Configs** (gestion des configurations d'alertes des charges de travail).

Sélectionnez le niveau de *Alert Severity* (gravité de l'alerte) et la *Disconnect Duration* (durée de la déconnexion) en minutes pour la configuration de l'alerte de l'orchestrateur externe.

Champ	Description
Gravité	Sélectionnez le niveau de gravité de cette règle :**LOW** (faible), **MEDIUM** (moyenne), **HIGH** (élevée), **CRITICAL** (critique) ou **IMMEDIATE ACTION** (Action immédiate)
Durée de la déconnexion (m)	La durée pendant laquelle une connexion est déconnectée.

Cliquez sur le bouton **Create** (créer) pour créer le nouvel orchestrateur externe, dont les détails de configuration peuvent être consultés en cliquant sur la ligne correspondante dans la vue de liste :

Figure 6: Détails de la configuration de l'orchestrateur externe

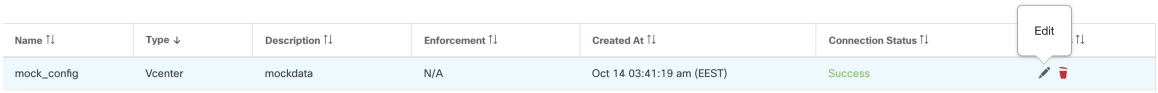


Note Étant donné que la première récupération complète d'instantané à partir d'un orchestrateur externe est une opération asynchrone, comptez environ une minute pour que le champ d'état de la connexion soit mis à jour.

Modifier un orchestrateur externe

Cliquez sur le bouton en forme de crayon à droite d'une ligne d'un orchestrateur externe, comme illustré ci-dessous, pour ouvrir une boîte de dialogue modale similaire à celle utilisée pour la création d'un orchestrateur externe, où la configuration peut être modifiée.

Figure 7: Modifier un orchestrateur externe



Note

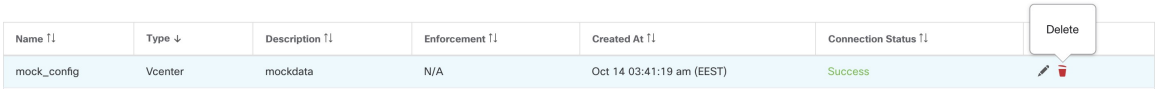
- Le champ **Type** n'est pas modifiable.
- Si une configuration utilise des clés ou des certificats pour l'authentification, les clés et les certificats doivent être fournis à chaque mise à jour de la configuration.
- Étant donné que les modifications de configuration d'un orchestrateur externe est réalisée de manière asynchrone, comptez environ une minute pour que le champ d'état de la connexion soit mis à jour et pour confirmer l'exactitude des modifications saisies.

Cliquez sur le bouton **Update** (mettre à jour) pour enregistrer les modifications apportées à la configuration.

Supprimer un orchestrateur externe

Caution La suppression d'un orchestrateur externe entraîne également la suppression des étiquettes fournies par cet orchestrateur, ce qui aura une incidence sur les politiques. Pour supprimer un orchestrateur externe, cliquez sur la corbeille comme indiqué ci-dessous :

Figure 8: Supprimer un orchestrateur externe



Étiquettes générées par l'orchestrateur

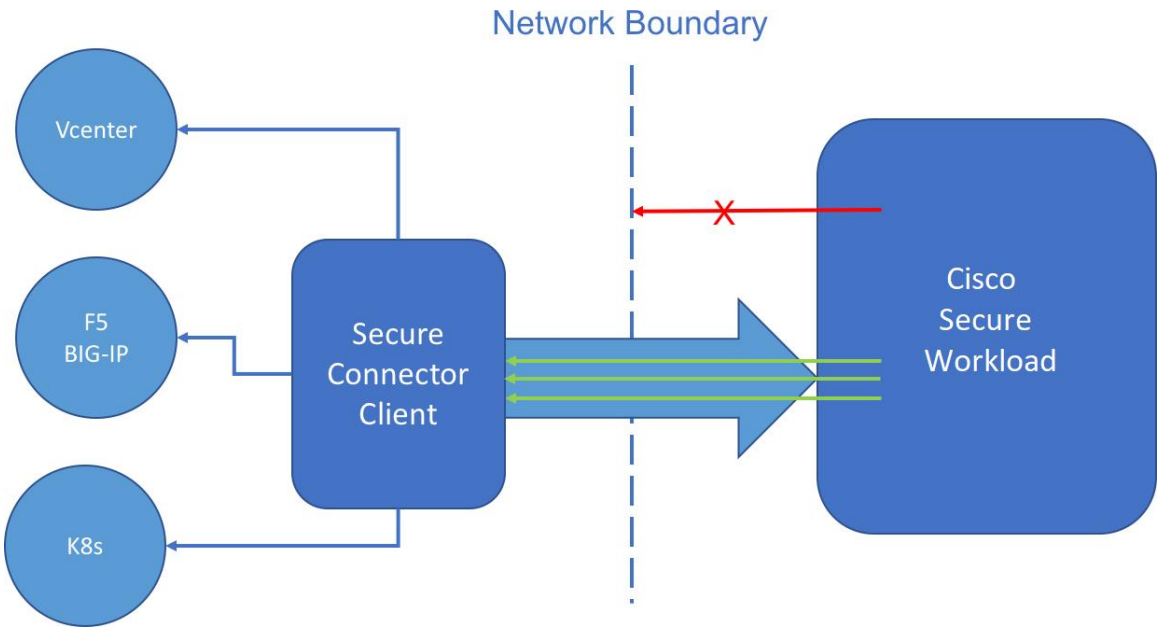
Cisco Secure Workload ajoute les étiquettes suivantes à toutes les instances AWS.

Clé	Valeur
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	*<Nom de la grappe Kubernetes>*
orchestrator_system/name	*<Nom du connecteur>*
orchestrator_system/cluster_id	*<UUID de la configuration de l'orchestrateur dans |produit|>*

Connecteur sécurisé

Pour que Cisco Secure Workload puisse importer des balises utilisateur ou appliquer des politiques sur les orchestrateurs externes (voir Orchestrateurs externes dans Cisco Secure Workload), Cisco Secure Workload doit établir des connexions sortantes vers les serveurs d'API des orchestrateurs (vCenter, Kubernetes, F5 BIG-IP, etc.). Parfois, il n'est pas possible d'autoriser les connexions entrantes directes vers les orchestrateurs à partir de la grappe Cisco Secure Workload. Le connecteur sécurisé résout ce problème en établissant une connexion sortante du même réseau que l'orchestrateur vers la grappe Cisco Secure Workload. Cette connexion est utilisée comme tunnel inverse pour renvoyer les demandes de la grappe au serveur d'API de l'orchestrateur.

Figure 9: Connecteur sécurisé



Pour chaque portée racine, un seul tunnel à la fois peut être actif. Les tentatives de démarrage de tunnels supplémentaires seront rejetées avec un message d'erreur indiquant qu'un tunnel est déjà actif. Le tunnel actif peut être utilisé pour se connecter à plusieurs orchestrateurs qui sont accessibles à partir du réseau dans lequel le client fonctionne. Une configuration par orchestrateur est utilisée pour indiquer si les connexions à cet orchestrateur doivent passer par le tunnel du connecteur sécurisé.

Toutes les communications entre le client Connecteur sécurisé et la grappe Cisco Secure Workload sont authentifiées et chiffrées mutuellement à l'aide de TLS.

Pour une sécurité accrue, il est conseillé aux clients d'installer le client Secure Connector (Connecteur sécurisé) sur un ordinateur isolé correctement sécurisé. L'ordinateur doit avoir des règles de pare-feu pour autoriser les connexions sortantes uniquement vers la grappe Cisco Secure Workload et tous les serveurs API externes de l'orchestrateur Cisco Secure Workload doivent être autorisés à y accéder.

Pour configurer les orchestrateurs en vue de l'utilisation du tunnel du connecteur sécurisé, consultez les instructions de configuration de l'orchestrateur externe pour votre produit.

Pour en savoir plus sur les points terminaux OpenAPI pour le connecteur sécurisé, consultez : Points d'accès d'API du connecteur sécurisé

Détails techniques

Pour amorcer le tunnel, le client connecteur sécurisé crée une paire de clés publique ou privée et signe son certificat de clé publique à distance par le serveur. Un jeton cryptographique à usage unique d'une durée limitée est utilisé pour sécuriser ce processus de signature à distance et pour identifier la portée racine à laquelle le client appartient. Du côté du serveur, chaque portée racine possède un certificat unique que le client utilise pour authentifier le serveur. Ces certificats sont régulièrement renouvelés pour assurer le secret de communication.

Le client connecteur sécurisé est composé d'un client de tunnel et d'un serveur SOCKS5. Une fois le tunnel démarré, le client attend les connexions par tunnellisation entrantes de la grappe Cisco Secure Workload. Les connexions entrantes sont gérées par le serveur SOCKS5 et transférées à l'hôte de destination.

Exigences relatives au client Connecteur sécurisé

Voici les exigences pour le client Connecteur sécurisé :

- RHEL ou CentOS 7 (x86_64)
- 2 cœurs de CPU
- 4 Go de RAM
- Une bande passante réseau suffisante pour gérer les données des orchestrateurs sur site qui utilisent le connecteur sécurisé.
- Connectivité sortante vers la grappe Cisco Secure Workload sur le port 443 (directe ou par l'intermédiaire d'un serveur mandataire HTTP(S)).
- Connectivité sortante vers les serveurs d'API Orchestrator internes (directe)

Déploiement client du connecteur sécurisé

Prise en charge de serveur mandataire

Le client du connecteur sécurisé prend en charge la connexion à la grappe Cisco Secure Workload par l'intermédiaire d'un serveur mandataire HTTP(S). Au besoin, le serveur mandataire doit être configuré en définissant la variable d'environnement HTTPS_PROXY pour le client. Pour définir la variable, ajoutez la ligne suivante dans la section *[Service]* du fichier de service systemd situé à l'emplacement */etc/systemd/system/tetration- secure-connector.service*. Ce paramètre ne sera pas conservé lors des réinstallations. Pour une configuration permanente, la ligne peut être ajoutée dans un nouveau fichier à l'adresse suivante */etc/systemd/system/tetration-secure-connector.service.d/10-https-proxy.conf*. Pour que l'une ou l'autre des configurations prenne effet, rechargez la configuration systemd en exécutant *systemctl daemon-reload*.

```
[Service]
Environment="HTTPS_PROXY=<Proxy Server Address>"
```

Présentation du déploiement

Le connecteur sécurisé crée un tunnel inverse de la grappe Cisco Secure Workload à votre réseau interne afin d'atteindre les serveurs d'API de votre orchestrateur.

Le démarrage du client du connecteur sécurisé nécessite le téléchargement du RPM Secure Connector et la génération d'un jeton d'enregistrement à usage unique.

1. Télécharger le dernier RPM du client du connecteur sécurisé sur une plateforme prise en charge.
2. Générer un jeton d'enregistrement.
3. Copier le jeton et démarrer le client sur l'hôte pour démarrer le client.

Déployer le client connecteur sécurisé

Télécharger le dernier RPM du client du connecteur sécurisé

Procédure

Étape 1 Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

Étape 2 Cliquez sur **Download Latest RPM** (Télécharger le dernier RPM).

Étape 3 Copiez l'ensemble RPM sur l'hôte Linux pour le déploiement, puis exécutez la commande suivante avec les privilèges racine :`rpm -ivh <rpm_filename>`.

Générer un jeton d'enregistrement

Procédure

Étape 1 Cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

Étape 2 Cliquez sur **Generate Registration Token** (Générer un jeton d'enregistrement).

Copier le jeton et démarrer le client

Après avoir généré un jeton d'enregistrement sur la page **Secure Connector** (connecteur sécurisé), vous obtiendrez un fichier *registration.token* (jeton d'enregistrement) qui contient le jeton à usage unique à durée limitée pour le démarrage du client. Arrêtez le client connecteur sécurisé sur l'hôte et copiez le fichier de jeton à l'emplacement où vous avez installé le paquet client connecteur sécurisé.

1. Pour arrêter le client, exécutez la commande suivante : `systemctl stop tetration-secure-connector`
2. Copiez le fichier *registration.token* dans le dossier `/etc/tetration/cert/`.
3. Pour redémarrer le client, exécutez la commande suivante : `systemctl start tetration-secure-connector`

[Facultatif] Déployer la version spécifique du client connecteur sécurisé

Procédure

Étape 1 Téléchargez une version précise du client connecteur sécurisé RPM.

a) Dans le volet de navigation, cliquez sur **Manage (Gestion)** > **Workloads (Charges de travail)** > **Agents (Agents)**.
b) Cliquez sur l'onglet **Installer** (Programme d' installation).
c) Cliquez sur **Manual Install using classic packaged installers (Installation manuelle à l'aide des programmes d'installation classiques)**, puis cliquez sur **Next** (suivant).

Les progiciels client connecteur sécurisé ont le type d'agent *Secure Connector* (Connecteur sécurisé).

d) Recherchez la version appropriée (si plusieurs sont disponibles sur la grappe) et cliquez sur **Download** (Télécharger).

e) Copiez l'ensemble RPM sur l'hôte Linux pour le déploiement, puis exécutez la commande suivante avec les privilèges racine :`rpm -ivh <rpm_filename>`.

Étape 2 Récupérez un nouveau jeton à l'aide de l'API.

Les jetons du connecteur sécurisé peuvent également être récupérés par le biais de l'OpenAPI (Get Tokenendpoint). Les extraits de code Python et Bash suivants peuvent être utilisés pour récupérer un nouveau jeton. Notez que la clé API utilisée doit avoir la capacité *external_integration* et avoir un accès en écriture à la portée racine spécifiée. Consultez la section OpenAPI Authentification (Authentification OpenAPI) pour obtenir des renseignements sur l'installation de OpenAPI client Cisco Secure Workload pour Python et la création d'une nouvelle clé API.

- **Fragment de code Python pour la récupération de jetons**

```
from tetpyclient import RestClient
from urllib import quote

API_ENDPOINT = "https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
ROOT_SCOPE_NAME = r"""<ROOT_SCOPE_NAME>"""
API_CREDENTIALS_FILE = "<API_CREDENTIALS_JSON_FILE>"
OUTPUT_TOKEN_FILE = "registration.token"

if __name__ == "__main__":
  client = RestClient(API_ENDPOINT,
                      credentials_file=API_CREDENTIALS_FILE)  # Add (verify=False) to
skip certificate verification
  escaped_root_scope_name = quote(ROOT_SCOPE_NAME, safe='')
  resp = client.get('/secureconnector/name/{}/token'.format(escaped_root_scope_name))
  if resp.status_code != 200:
    print 'Error ({}): {}'.format(resp.status_code, resp.content)
    exit(1)
  else:
    with open(OUTPUT_TOKEN_FILE, 'w') as f:
      f.write(resp.content)
```

- **Fragment de code BASH pour la récupération de jetons**

```
#!/bin/bash
HOST="https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
API_KEY="<API_KEY>"
API_SECRET="<API_SECRET>"
ROOTSCOPE_NAME="<ROOT_SCOPE_NAME>" # if the name contains spaces or special characters,
 it should be url-encoded
TOKEN_FILE="registration.token"
INSECURE=1 # Set to 0 if you want curl to verify the identity of the cluster

METHOD="GET"
URI="/openapi/v1/secureconnector/name/$ROOTSCOPE_NAME/token"
CHK_SUM=""
CONTENT_TYPE=""
TS=$(date -u "+%Y-%m-%dT%H:%M:%S+0000")
CURL_ARGS="-v"
if [ $INSECURE -eq 1 ]; then
    CURL_ARGS=$CURL_ARGS" -k"
fi
```

```
    MSG=$(echo -n -e "$METHOD\n$URI\n$CHK_SUM\n$CONTENT_TYPE\n$TS\n")
   SIG=$(echo "$MSG"| openssl dgst -sha256 -hmac $API_SECRET -binary | openssl enc -base64)

    REQ=$(echo -n "curl $CURL_ARGS $HOST$URI -w '%{http_code}' -H 'Timestamp: $TS' -H 'Id:
$API_KEY' -H 'Authorization: $SIG' -o $TOKEN_FILE")
    status_code=$(sh -c "$REQ")
    if [ $status_code -ne 200 ]; then
        echo "Failed to get token. Status: " $status_code
    else
        echo "Token retrieved successfully"
    fi
```

Étape 3 Copier le jeton et démarrer le client. Pour plus de renseignements sur les instructions, consultez Copier le jeton et démarrer le client, à la page 12.

Vérifier l'état du client connecteur sécurisé

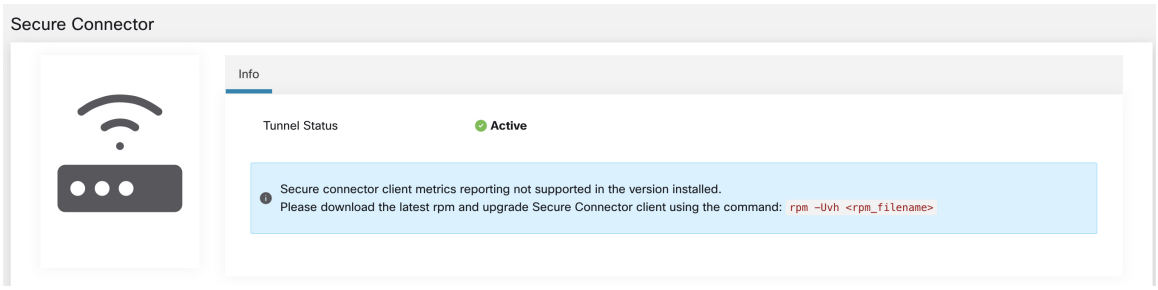
- Pour vérifier si le client Connecteur sécurisé est installé, interrogez la base de données RPM pour trouver le paquet *tet- secureconnector-client-site* en exécutant la commande suivante : `rpm -q tet-secureconnector-client-site`
- Pour vérifier l'état du client installé, vous pouvez vérifier l'état du service *tetration-secure-connector* systemd en exécutant la commande suivante : `systemctl status tetration-secure-connector`

État du client du connecteur sécurisé

Dans la page **External Orchestrateurs**, l'état des orchestrateurs externes configurés et du tunnel du connecteur sécurisé s'affiche. Si le connecteur sécurisé est activé lors de la configuration des orchestrateurs externes, vous pouvez afficher les métriques du client **Secure Connector** dans la page Secure Connector (connecteur sécurisé).

Cependant, si l'état du tunnel de Cisco Secure Connector est **Actif** mais que les métriques du client ne sont pas visibles, cela signifie qu'une version plus ancienne de Cisco Secure Connector est installée. Un message de mise à niveau dans la version de Secure Connector Client s'affiche comme suit :

Figure 10: Message de mise à niveau du client de connecteur sécurisé



Note Pour obtenir des instructions sur l'installation du dernier RPM client du connecteur sécurisé, consultez la section Télécharger le dernier RPM du client du connecteur sécurisé.

Pour afficher les mesures du client :

Procedure

Étape 1 Sous **Configure Details** (Détails de la configuration), cliquez sur la ligne **Status** (État). La page **Secure Connector** (Connecteur sécurisé) s'affiche.

Note Pour accéder à l'état du tunnel Secure Connector, sélectionnez **Manage (Gestion)** > **Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)** dans le volet gauche.

Étape 2 Sélectionnez les onglets **General** (General), **Interface** (Interface) ou **Routes** (routes) pour accéder à plus de détails sur l'état de la connectivité entre le client et la grappe Cisco Secure Workload.

Onglets	Description
Généralités	Répertorie les informations suivantes : • État du tunnel • Nom d'hôte • Adresse IP • Mandataire HTTP/HTTPS • Version : répertorie la version du build. • Nb de vCPU • Mémoire totale (Go) • Disponibilité : répertorie la disponibilité de la machine virtuelle sur laquelle le client du connecteur sécurisé est exécuté. • Last heartbeat Received (dernière pulsation reçue) : indique le jour et l'horodatage de la dernière pulsation reçue du client. • Nb d'échecs de pulsation (dernier jour) : indique le nombre d'échecs de la connectivité au client connecteur sécurisé au cours de la journée. Si le client reste inactif, le nombre n'est pas incrémenté. Le compte est réinitialisé à la fin de la journée. • Latence aller-retour (ms)
Interface	Répertorie les détails de l'interface de la machine virtuelle sur laquelle le client connecteur sécurisé est exécuté.

Onglets	Description
Routes	La table de routage répertorie les adresses IP de destination, la passerelle, le masque de génération et l'interface.

Alertes du connecteur sécurisé

L'alerte est générée lorsque le connecteur sécurisé cesse de fonctionner ou en l'absence de pulsations au cours de la dernière minute.

Étape 1 : Pour activer l'alerte, cliquez sur **Manage (Gestion) Workloads (Charges de travail)** > **Secure Connector (Connecteur sécurisé)**.

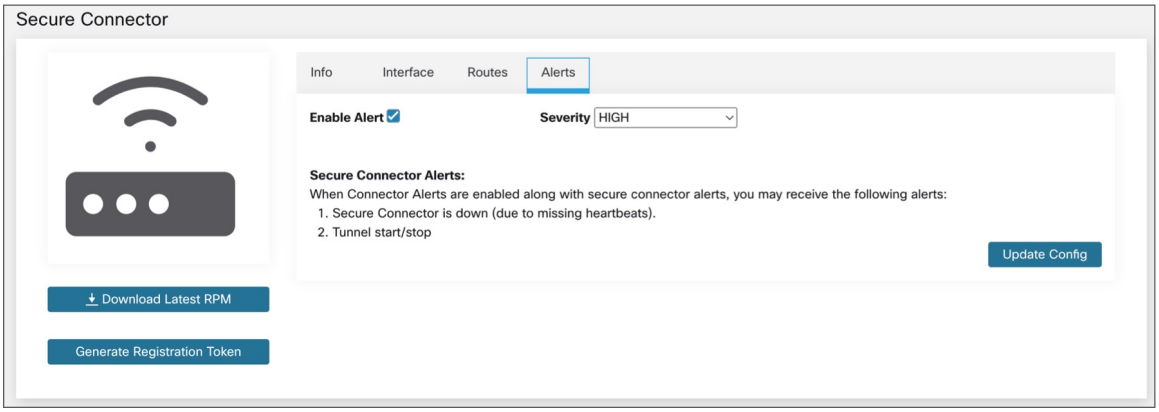
Étape 2 : Cliquez sur l'onglet **Alerts** (alertes).

Étape 3 : Cochez la case **Enable Alert** (activer l'alerte).

Étape 4 : Choisissez une valeur de **Severity** (gravité) dans le menu déroulant.

Étape 5 : Cliquez sur **Update Config** (Mettre à jour la configuration).

Illustration 11 : Activer les alertes du connecteur sécurisé



Remarque Assurez-vous que les alertes des connecteurs sont activées dans la page **Manage (Gestion)** > **Alerts - Configuration Configuration des alertes)**.

Accédez à **Investigate** (Enquêter) > **Alerts** (Alertes) et cliquez sur une alerte pour en savoir plus.

Texte d'alerte : : Secure Connector(connecteur sécurisé) : <motif de l'échec de la connexion>

Illustration 12 : Alerte du connecteur sécurisé

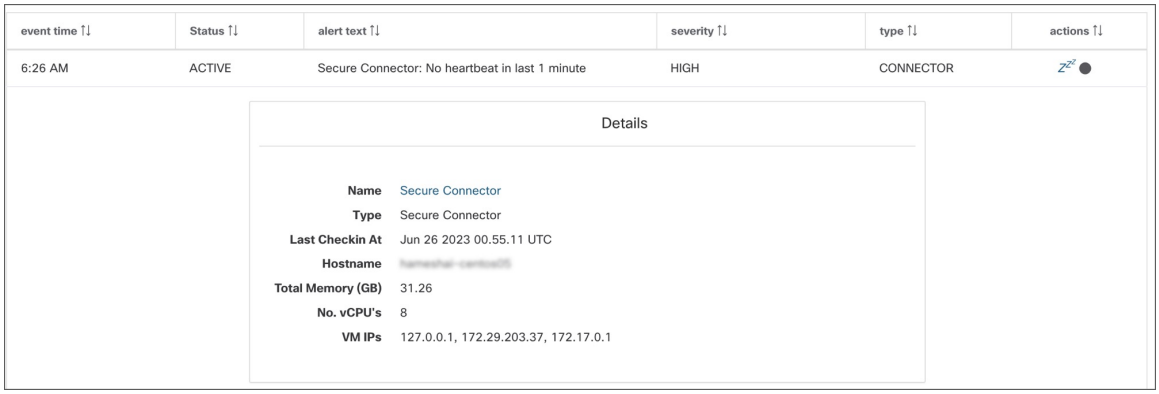


Tableau 2 : Détails de l'alerte

Champ	Type	Description
Nom	Chaîne	Nom du connecteur sécurisé
Type	Chaîne	Type du connecteur sécurisé
Last Checkin At	Chaîne	Dernière heure connue de pulsation
Hostname (Nom d'hôte)	Chaîne	Nom de la machine hébergeant ce connecteur sécurisé
Total Memory (GB)	Chaîne	RAM en Go
No. vCPU's	Chaîne	Nombre de CPU
VM IPs	Chaîne	Liste des interfaces réseau sur l'hôte client du connecteur sécurisé

Mettre à niveau le client connecteur sécurisé

Le client Secure Connector (Connecteur sécurisé) ne prend pas en charge les mises à jour automatiques. Pour déployer une nouvelle version :

1. Exécutez la commande suivante pour désinstaller la version actuelle : `rpm -e tet-secureconnector-client-site`
2. Déployez la nouvelle version. Pour plus de renseignements sur les instructions, consultez Déployer le client connecteur sécurisé, on page 12.

Désinstaller le client connecteur sécurisé

Le client connecteur sécurisé peut être désinstallé à l'aide de la commande suivante `rpm -e tet-secureconnector-client-site`

Amazon Web Services

Note La fonctionnalité d'orchestrateur externe d'AWS fait désormais partie de la nouvelle fonctionnalité de connecteur infonuagique AWS. Si vous avez effectué une mise à niveau vers cette version, vos orchestrateurs externes AWS existants sont maintenant en lecture seule; si vous devez apporter des modifications, créez un nouveau connecteur AWS. Pour en savoir plus, consultez Connecteur AWS.

Cisco Secure Workload prend en charge l'acquisition automatisée de l'inventaire en direct à partir d'une région AWS. Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « aws », l'appareil Cisco Secure Workload se connecte au point terminal AWS et récupère les métadonnées pour toutes les instances à l'état d'exécution ou d'arrêt.

Prérequis

- Les jetons de sécurité (clé d'accès et clé secrète) utilisés doivent avoir le type de privilèges IAM approprié pour permettre la récupération des informations de l'orchestrateur.

Champs de configuration

Attribut	Description
Identifiant	Identifiant unique de l'orchestrateur.
Nom	Nom spécifié par l'utilisateur de l'orchestrateur.
Type	Type d'orchestrateur - (*aws* dans ce cas)
Description	Une brève description de l'orchestrateur.
ID de la clé d'accès AWS	CLÉ D'ACCÈS associée au compte pour lequel la configuration de l'orchestrateur est en cours de création.
Clé d'accès secrète AWS	CLÉ SECRÈTE associée au compte que vous créez pour la configuration de l'orchestrateur. **Note** Saisissez à nouveau la clé secrète si vous modifiez la configuration de l'orchestrateur.
Région AWS	La région dans laquelle la charge de travail a été déployée. Si une charge de travail est répartie sur plusieurs régions, une configuration distincte est requise pour chaque région. Consultez le lien ci-dessous pour connaître les valeurs de *région* correctes. :ref:https://docs.aws.amazon.com/general/latest/gr/rande.html.

Attribut	Description
Accept Self-signed Cert (Accepter le certificat autosigné)	Est automatiquement marqué comme vrai pour AWS. L'utilisateur ne peut pas le modifier.
Intervalle complet entre les instantanés	Intervalle de l'instantané complet en secondes. Le gestionnaire d'inventaire de l'orchestrateur effectuera une interrogation d'actualisation complète à partir de l'orchestrateur.
Intervalle différentiel entre les instantanés	Intervalle de l'instantané différentiel en secondes. Le gestionnaire d'inventaire de l'orchestrateur récupérera uniquement les mises à jour incrémentielles de l'orchestrateur.
Liste d'hôtes	Le type d'orchestrateur AWS ne nécessite pas de liste d'hôtes. Le point terminal pour AWS sera dérivé du champ *AWS Region* (région AWS) ci-dessus. Ce champ doit être laissé vide.
Mesures TSDB détaillées	Si cette option est activée, les mesures tsdb pour chaque orchestrateur individuel seront rapportées. Sinon, une agrégation de toutes les mesures de l'orchestrateur sera rapportée.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Tunneliser les connexions vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel de Connecteur sécurisé.

Flux de travaux

- Configurez un orchestrateur AWS avec les champs de configuration ci-dessus.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes suivantes à toutes les instances AWS.

Clé	Valeur
orchestrator_system/orch_type	AWS
orchestrator_system/cluster_name	<*Nom de la grappe Kubernetes*>
orchestrator_system/name	<*Nom du connecteur*>
orchestrator_system/cluster_id	<*UUID de la configuration de l'orchestrateur dans |produit|*>

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à l'instance.

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*<Numéro d'instance attribué par AWS>*
orchestrator_system/machine_name	*<PublicDNS(nom de domaine complet (FQDN)) donné à ce nœud par AWS>*
orchestrator_‘<Clé d'étiquette AWS>‘	*<Valeur de l'étiquette AWS>*

Dépannage

- Confusion entre la région AWS et la zone de disponibilité

  Ces deux valeurs sont interdépendantes et ne doivent pas être confondues. Par exemple, us-ouest-1 pourrait être la région et la zone de disponibilité peut être us-ouest-1a ou us-ouest-1b, etc. Lors de la configuration de l’orchestrateur, la *région* doit être utilisée. Reportez-vous à https://docs.aws.amazon.com/general/latest/gr/rande.html pour toutes les régions.

- Problème de connectivité et de renseignements d’authentification après la mise à jour de la configuration de l’orchestrateur

  Les clients doivent soumettre de nouveau la *clé secrète AWS* chaque fois que la configuration est mise à jour.

Kubernetes/OpenShift

Note Les fonctionnalités des orchestrateurs externes EKS et AKS font désormais partie des nouvelles fonctionnalités des connecteurs infonuagiques AWS et Azure, respectivement. Si vous avez effectué la mise à niveau vers cette version, vos orchestrateurs externes EKS et AKS existants sont maintenant en lecture seule; si vous devez apporter des modifications, créez un nouveau connecteur AWS ou Azure. Pour des renseignements complets, consultez les rubriques pertinentes sous Connecteurs pour l'informatique infonuagique.

L’orchestrateur externe pour Kubernetes et OpenShift standard n’a pas été modifié.

Cisco Secure Workload prend en charge l’acquisition automatisée de l’inventaire en direct à partir d’une grappe Kubernetes. Lorsqu’une configuration d’orchestrateur externe est ajoutée pour une grappe Kubernetes/OpenShift, Cisco Secure Workload se connecte au serveur d’API de la grappe et suit l’état des nœuds, des pods et des services dans cette grappe. Pour chaque type d'objet, Cisco Secure Workload importe toutes les étiquettes Kubernetes et les étiquettes associées à l'objet. Toutes les valeurs sont importées en l'état.

En plus d’importer les étiquettes définies pour les objets Kubernetes/OpenShift, Cisco Secure Workload génère également des étiquettes qui facilitent l’utilisation de ces objets dans les filtres d’inventaire. Ces étiquettes supplémentaires sont particulièrement utiles pour définir les portées et les politiques.

Pour en savoir plus sur toutes ces étiquettes, consultez Étiquettes relatives aux grappes Kubernetes.

Si l'application est activée sur les nœuds Kubernetes (les agents d'application sont installés et le profil de configuration active l'application sur ces agents), les politiques d'application seront installées à la fois sur les

nœuds et à l'intérieur des espaces de noms des pods en utilisant les informations acquises sur les entités Kubernetes par le biais de cette intégration.

À propos de Kubernetes sur les plateformes infonuagiques

Pour les services Kubernetes gérés suivants qui s'exécutent sur des plateformes infonuagiques prises en charge, la fonctionnalité de cet orchestrateur est fournie à l'aide de connecteurs infonuagiques :

- Elastic Kubernetes Service (EKS) s'exécutant sur Amazon Web Services (AWS)
- Azure Kubernetes Service (AKS) s'exécutant sur Microsoft Azure
- Google Kubernetes Engine (GKE) s'exécutant sur Google Cloud Platform (GCP)

Pour plus de détails sur l'obtention de données à partir de grappes Kubernetes sur les plateformes infonuagiques, consultez les rubriques sous Connecteurs infonuagiques.

Exigences et prérequis

- Pour les versions de Kubernetes et d'OpenShift prises en charge, consultez https://www.cisco.com/go/secure-workload/requirements/integrations
- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité.

Champs de configuration

Les champs de configuration suivants concernent la configuration de l'orchestrateur Kubernetes dans l'objet Orchestrateur.

Champ	Description
Nom	Nom de l'orchestrateur spécifié par l'utilisateur.
Description	Description de l'orchestrateur précisée par l'utilisateur.
Intervalle différentiel	Intervalle (en secondes) pour vérifier les modifications sur le point terminal Kubernetes
Intervalle complet entre les instantanés	Intervalle (en secondes) pour effectuer un instantané complet des données Kubernetes
Username	Nom d'utilisateur pour le point terminal de l'orchestration.
Mot de passe	Mot de passe du point terminal de l'orchestration.
Certificat	Votre certificat client servira à l'authentification.
Clé	Clé correspondant au certificat client.
Jeton d'authentification	Jeton d'authentification opaque (jeton porteur).

Champ	Description
Certificat de l'autorité de certification	Certificat de l'autorité de certification pour valider le point terminal de l'orchestration.
Accept Self-signed Cert (Accepter le certificat autosigné)	Case pour désactiver la vérification SSL stricte du certificat du serveur d'API Kubernetes
Mesures TSDB détaillées	Maintenir les mesures par Kubernetesorchestrator – si la valeur est Faux (False), seules les mesures à l'échelle de la grappe Cisco Secure Workload sont conservées.
Secure Connector Tunnel (Tunnel du connecteur sécurisé)	Connexions de tunnel vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel du connecteur sécurisé
Liste d'hôtes	Tableau de paires { « host_name », « port_number »,} (nom de l'hôte, numéro de port) qui précisent comment Cisco Secure Workload doit se connecter à l'orchestrateur
Type de gestionnaire K8	Type de gestionnaire pour la grappe Kubernetes (aucun pour les déploiements standard/OpenShift Kubernetes)
Nom de la grappe AWS	Nom de l'orchestrateur comme spécifié au moment de la création de la grappe (EKS préexistant)
ID d'accès AWS	CLÉ D'ACCÈS associée au compte pour lequel la configuration de l'orchestrateur est créée (EKS préexistant)
Clé d'accès secrète AWS	La CLÉ SECRÈTE associée au compte pour lequel la configuration de l'orchestrateur est créée. Saisissez à nouveau la clé secrète chaque fois que la configuration est modifiée. (EKS pré-existant)
Région AWS	La région dans laquelle la charge de travail a été déployée. Si une charge de travail est répartie sur plusieurs régions, une configuration distincte est requise pour chaque région. Consultez le lien ci-dessous pour connaître les valeurs de *région* correctes. :ref: https://docs.aws.amazon.com/general/latest/gr/rande.html. (EKS pré-existant)
ARN Assume Role AWS	Numéro de ressource Amazon des rôles à assumer lors de la connexion à l'outil d'orchestration : https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html (EKS préexistant)

Champ	Description
ID du détenteur Azure	Identifiant du détenteur associé à l'abonnement Azure. (AKS pré-existant uniquement)
ID du client Azure	Identifiant global unique associé à l'application qui doit s'authentifier auprès d'Azure AD. (AKS pré-existant uniquement)
Code secret du client Azure	Mot de passe associé au principal service pour l'application qui doit s'authentifier auprès d'Azure AD. (AKS pré-existant uniquement)

Règles d'or de l'orchestrateur

Les attributs d'objet des règles d'or sont décrits ci-dessous. Ces règles d'or permettent de préciser les règles nécessaires à la grappe Kubernetes pour rester fonctionnelle une fois que la mise en application est activée sur les nœuds de la grappe Kubernetes.

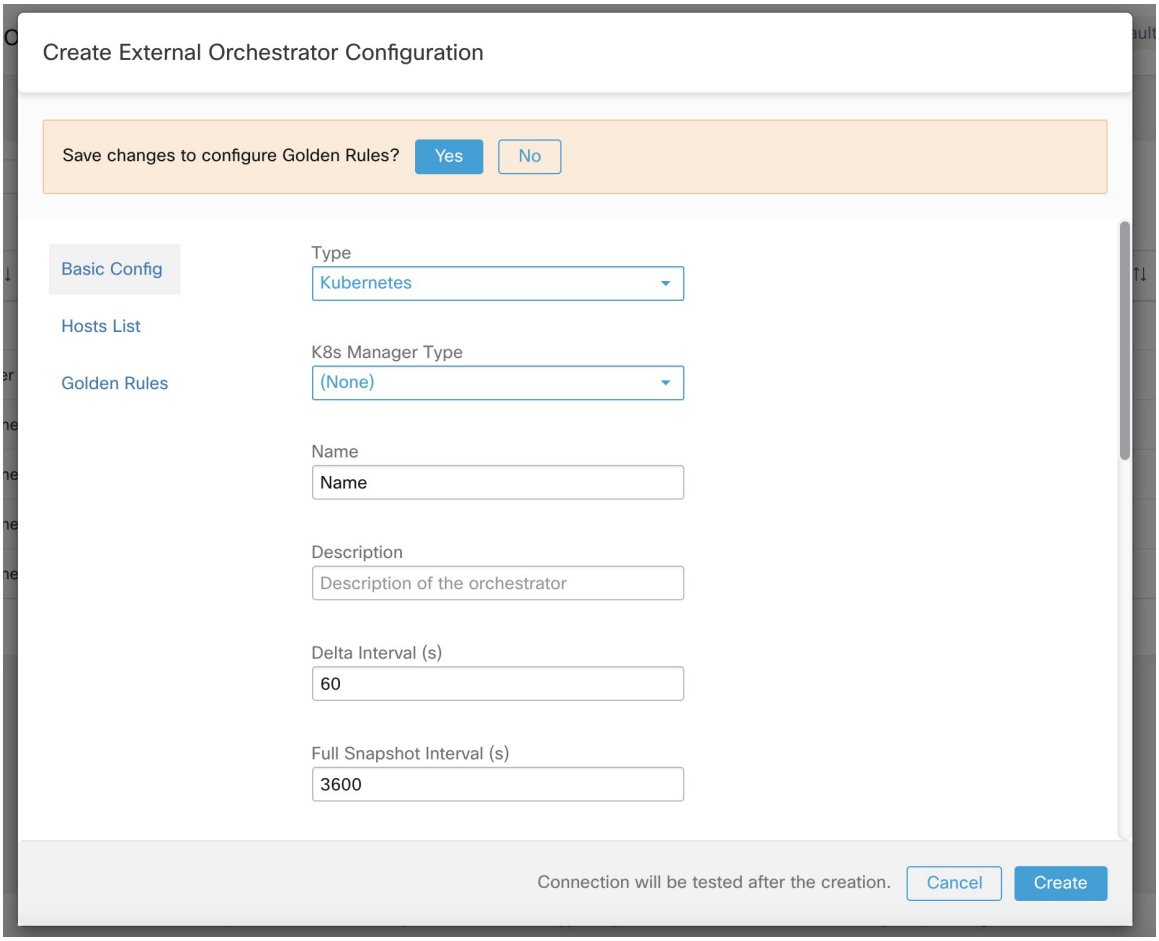
Attribut	Description
Port Kubelet	Port d'API local au nœud de Kubelet
Services	Tableau d'objets des services Kubernetes

Le port Kubelet est nécessaire pour créer des politiques autorisant le trafic des daemons de gestion Kubernetes vers les kubelets, par exemple pour les journaux en direct, les exécutions de pods en mode interactif, etc. La connectivité vitale entre les différents services et daemons Kubernetes est spécifiée sous la forme d'une série de services - chaque entrée du tableau de services a la structure suivante :

- Description : une chaîne qui décrit le service.
- Adresses : une liste d'adresses de points terminaux de service du format <IP>:<port> /<protocol>.
- Consommé par : une liste des consommateurs des points terminaux (les valeurs autorisées sont les pods ou les nœuds)

Note Si **Kubernetes** est choisi comme type, la configuration des règles d'or sera autorisée.

Figure 13: Créer une configuration de règles d'or pour le type Kubernetes



Flux de travaux

- Configurez le tunnel du connecteur sécurisé, si nécessaire, pour la connectivité de la grappe Cisco Secure Workload à un serveur ou des serveurs d'API Kubernetes.
- Configurez un orchestrateur Kubernetes rempli avec les champs de configuration ci-dessus.
- Configurez les règles d'or pour l'orchestrateur Kubernetes.

Considérations relatives aux ressources pour le contrôle d'accès en fonction des rôles (Role-Based Access Control ou RBAC) de Kubernetes

Le client Kubernetes tente de RECEVOIR/RÉPERTORIER/SURVEILLER les ressources suivantes. Il est fortement recommandé de NE PAS configurer la clé ou le certificat d'administrateur ou un compte de service administrateur.

Les informations d'authentification Kubernetes fournies doivent avoir un ensemble minimal de privilèges sur les ressources suivantes :

Ressources	Verbes Kubernetes
points terminaux	[obtenir la liste de surveillance]
espaces de noms	[obtenir la liste de surveillance]
nodes	[obtenir la liste de surveillance]
pods	[obtenir la liste de surveillance]
services	[obtenir la liste de surveillance]
entrées	[obtenir la liste de surveillance]
contrôleurs de duplication	[obtenir la liste de surveillance]
jeux de répliques	[obtenir la liste de surveillance]
déploiements	[obtenir la liste de surveillance]
daemonsets	[obtenir la liste de surveillance]
statefulsets	[obtenir la liste de surveillance]
tâches	[obtenir la liste de surveillance]
cronjobs	[obtenir la liste de surveillance]

En substance, vous pouvez créer un compte de service spécial sur votre serveur Kubernetes avec ces privilèges minimaux. Vous trouverez ci-dessous un exemple de séquence de commandes kubectl qui facilitera la création de ce compte de service. Notez l'utilisation de clusterrole (non de rôle) et clusterrolebindings (non de rolebindings) - ce sont des rôles à l'échelle de la grappe et non d'un espace de nom. L'utilisation d'une liaison de rôle ou de rôle ne fonctionnera pas, car Cisco Secure Workload tente de récupérer les données de tous les espaces de noms.

```
$ kubectl create serviceaccount csw.read.only
```

Créez le rôle de grappe (clusterrole).

Un exemple de fichier clusterrole.yaml avec des privilèges minimaux est fourni ci-dessous.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: csw.read.only
rules:
  - apiGroups:
    - ""
    resources:
      - nodes
      - services
      - endpoints
      - namespaces
      - pods
      - replicationcontrollers
      - ingresses
    verbs:
      - get
```

```
      - list
      - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
    resources:
      - ingresses
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - apps
    resources:
      - replicasets
      - deployments
      - statefulsets
      - daemonsets
    verbs:
      - get
      - list
      - watch
  - apiGroups:
    - batch
    resources:
      - jobs
      - cronjobs
    verbs:
      - get
      - list
      - watch

$ kubectl create -f clusterrole.yaml
```

Note Les groupes d'API pour ces différentes ressources sont susceptibles de changer selon les versions de Kubernetes. L'exemple ci-dessus devrait fonctionner pour les versions 1.20 à 1.24 de Kubernetes et pourrait nécessiter quelques ajustements pour d'autres versions.

Créer la liaison de rôles de grappe

```
$ kubectl create clusterrolebinding csw.read.only --clusterrole=csw.read.
‹→only --serviceaccount=default:csw.read.only
```

Pour récupérer le code secret authtoken du compte de service (utilisé dans le champ Auth Token dans l'interface graphique) et le décoder en base64, vous pouvez récupérer le nom du code secret en listant le compte de service avec la sortie yaml.

```
$ kubectl get serviceaccount -o yaml csw.read.only
apiVersion: v1
kind: ServiceAccount
metadata:
  creationTimestamp: 2020-xx-xxT19:59:57Z
  name: csw.read.only
  namespace: default
  resourceVersion: "991"
  selfLink: /api/v1/namespaces/default/serviceaccounts/e2e.minimal
  uid: ce23da52-a11d-11ea-a990-525400d58002
secrets:
- name: csw.read.only-token-vmvmz
```

Lister le code secret en mode de sortie yaml produira le jeton mais au format Base64 (ce qui est la procédure standard de Kubernetes pour les données secrètes). Cisco Secure Workload n'accepte pas le jeton dans ce format, vous devez le décoder à partir de Base64.

```
$ kubectl get secret -o yaml csw.read.only-token-vmvmz
apiVersion: v1
data:
  ca.crt: ...
  namespace: ZGVmYXVsdA==
  token: ZXlKaGJHY2lPaUpTVX....HRfZ2JwMVZR
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: csw.read.only
    kubernetes.io/service-account.uid: ce23da52-a11d-11ea-a990-525400d58002
  creationTimestamp: 2020-05-28T19:59:57Z
  name: csw.read.only-token-vmvmz
  namespace: default
  resourceVersion: "990"
  selfLink: /api/v1/namespaces/default/secrets/csw.read.only-token-vmvmz
  uid: ce24f40c-a11d-11ea-a990-525400d58002
type: kubernetes.io/service-account-token
```

Pour répertorier le code secret et afficher uniquement le champ `.data.token` et décoder le codage en base 64 en une seule commande, la commande suivante qui utilise l'option `--template` est utile.

```
  $ kubectl get secret csw.read.only-token-vmvmz --template "{{ .data.token }}" | base64
-d
```

Cet authtoken peut être utilisé pour configurer un orchestrateur Kubernetes dans l'interface utilisateur Cisco Secure Workload au lieu de nom d'utilisateur/mot de passe ou de clé/certificat.

Consultez la section Considérations relatives à RBAC EKS.

Étiquettes générées par l'orchestrateur

Consultez la section Étiquettes liées aux grappes Kubernetes.

Dépannage

- Analyse ou incompatibilité des informations d'authentification de la clé ou du certificat client

  Celles-ci doivent être fournies au format PEM et correspondre à l'entrée correcte du fichier kubectl.conf. Nous avons rencontré des clients qui collaient des certificats d'autorité de certification dans les champs de certificats des clients, ainsi que des clés et des certificats qui ne correspondaient pas les uns aux autres.

- Identifiants Gcloud au lieu des identifiants GKE

  Les clients qui utilisent GKE sous la ligne de commande gcloud fournissent par erreur les informations d'authentification gcloud alors que les informations d'authentification de grappe GKE sont nécessaires.

- Version de la grappe Kubernetes non prise en charge

  L'utilisation d'une version incompatible de Kubernetes peut entraîner des défaillances. Vérifiez que la version de Kubernetes figure dans la liste des versions prises en charge.

- Les informations d'authentification ont des privilèges insuffisants

Vérifiez que le jeton d'authentification ou la clé d'utilisateur client, ou le certificat utilisé dispose de tous les privilèges répertoriés dans le tableau ci-dessus.

- L'inventaire Kubernetes n'en finit pas de basculer

  Le champ hosts_list spécifie un groupe de serveurs d'API pour la même grappe Kubernetes – vous ne pouvez pas l'utiliser pour configurer plusieurs grappes Kubernetes. Cisco Secure Workload vérifiera la réactivité et sélectionnera aléatoirement l'un de ces points terminaux pour s'y connecter et récupérer les informations de l'inventaire Kubernetes. Aucun équilibrage de charge n'est effectué ici, et il n'y a aucune garantie de répartition uniforme de la charge sur ces points terminaux. S'il s'agit de grappes différentes, l'inventaire de Kubernetes continuera à basculer entre elles, selon le serveur d'API de la grappe auquel nous nous connectons.

- Plusieurs méthodes d'autorisation

  Plusieurs méthodes d'autorisation peuvent être saisies lors de la configuration (nom d'utilisateur ou mot de passe, authtoken, clé ou certificat client) et seront utilisées dans la connexion client établie avec le serveur d'API. Les règles standard de Kubernetes concernant les méthodes d'autorisation simultanée valides s'appliquent ici.

- La validation du certificat SSL échoue

  Si le point de terminaison de l'API Kubernetes se trouve derrière un NAT ou un équilibreur de charge, le numéro de répertoire (NR) dans le certificat SSL généré sur les nœuds du plan de contrôle Kubernetes peut ne pas correspondre à l'adresse IP configurée dans Cisco Secure Workload. Cela entraînera un échec de validation SSL même si le certificat de l'autorité de certification est fourni et valide. Le bouton Insecure (Non sécurisé) contourne la validation stricte des certificats SSL du serveur et aidera à contourner ce problème, mais peut entraîner des problèmes de MITM. Le correctif correct consiste à modifier le certificat de l'autorité de certification pour fournir des entrées SAN (Subject Alternative Name) pour toutes les entrées DNS ou IP qui peuvent être utilisées pour se connecter à la grappe Kubernetes.

VMware vCenter

L'intégration de vCenter permet à l'utilisateur de récupérer les attributs sans système d'exploitation et de machine virtuelle du vCenter configuré.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « vCenter », Cisco Secure Workload récupère les attributs de machines sans système d'exploitation et de VM pour toutes les machines sans système d'exploitation et les machines virtuelles contrôlées par cette instance de vCenter. Cisco Secure Workload importera les attributs suivants d'une machine virtuelle ou d'une machine sans système d'exploitation : a) le nom d'hôte b) les adresses IP c) l'UUID BIOS d) les catégories/étiquettes.

Un nouvel inventaire sera créé dans Cisco Secure Workload avec les attributs de machines sans système d'exploitation et des machines virtuelles ci-dessus, si l'inventaire n'est pas présent dans l'appareil. Si l'inventaire est déjà présent dans l'appareil (créé par le capteur de visibilité Cisco Secure Workload fonctionnant sur l'ordinateur sans système d'exploitation/la machine virtuelle), l'inventaire existant sera étiqueté avec la liste des catégories/étiquettes d'ordinateurs sans système d'exploitation/de VM récupérés.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité.
- La version de vCenter prise en charge est la 6.5+

Champs de configuration

En plus des champs de configuration courants, décrits dans la section *Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

- **La liste des hôtes** est un tableau de paires de noms d'hôte/adresse IP et de ports pointant vers le serveur vCenter à partir duquel les attributs de machines sans système d'exploitation/de machines virtuelles seront extraits.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur vCenter est accessible sur cette adresse IP/ce port à partir de la grappe Cisco Secure Workload.
- Pour TaaS ou dans les cas où le serveur vCenter n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes suivantes à toutes les machines virtuelles apprises du serveur vCenter.

Clé	Valeur
orchestrator_system/orch_type	vCenter
orchestrator_system/cluster_name	*<Nom donné à la configuration de cette grappe>*
orchestrator_system/cluster_id	*<L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload>*

Étiquettes spécifiques à l'instance

Les étiquettes suivantes sont propres à l'instance.

Table 3: Les étiquettes suivantes sont propres à l'instance.

Clé	Valeur
orchestrator_system/workload_type	vm
orchestrator_system/machine_id	*UUID BIOS de machine sans système d'exploitation/VM*
orchestrator_system/machine_name	*Nom d'hôte de la machine sans système d'exploitation/de la machine virtuelle*
orchestrator_'<Category Name>'	*<Tag Value>*

Mises en garde

- Lorsqu'une configuration d'orchestrateur externe est ajoutée à vCenter, le logiciel Cisco Secure Workload se connecte au serveur vCenter spécifié dans la liste d'hôtes. Une fois la connexion au serveur réussie, le logiciel Cisco Secure Workload importera les noms d'hôte, les adresses IP et les catégories ou étiquettes pour toutes les machines sans système d'exploitation et les machines virtuelles présentes sur le serveur vCenter. Pour importer les noms d'hôte et les adresses IP de la machine sans système d'exploitation et des machines virtuelles, les outils de VM doivent être installés sur l'ensemble de la machine sans système d'exploitation et les machines virtuelles. Si les outils VM ne sont pas installés pour une machine virtuelle ou sans système d'exploitation, le logiciel Cisco Secure Workload n'affichera pas les catégories ou les étiquettes pour cette machine virtuelle ou sans système d'exploitation en particulier.
- Le logiciel Cisco Secure Workload n'importe pas les attributs personnalisés du logiciel sans système d'exploitation ou de la machine virtuelle.
- Il est recommandé de fixer la durée de minuterie de l'intervalle **Delta** à plus de 10 minutes afin de réduire la charge sur le serveur vCenter. Toute modification de l'inventaire ou des étiquettes sur le serveur vCenter aura un délai de propagation d'au moins 10 min, une fois la minuterie mentionnée ci-dessus modifiée.

Dépannage

- Problèmes de connexion

  Si le dispositif Cisco Secure Workload ne peut pas se connecter ou atteindre le serveur vCenter, l'onglet **Connection Status** (État de la connexion) de l'orchestrateur externe affichera l'état de l'échec ainsi que l'erreur appropriée, le cas échéant.

- Contrôle de l'intégrité du logiciel Cisco Secure Workload.

  Consultez la page **MAINTENANCE/Service Status** (MAINTENANCE/état de service) pour voir si un service est en panne. Vérifiez si **OrchestratorInventoryManager** est opérationnel et fonctionne.

DNS

L'intégration du DNS permet à Cisco Secure Workload d'annoter un inventaire connu avec des renseignements DNS tels que les noms d'hôte des enregistrements CNAME et A/AAAA.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « dns », l'appareil Cisco Secure Workload tente de se connecter au(x) serveur(s) DNS et effectue un téléchargement de transfert de zone des enregistrements DNS. Ces enregistrements (uniquement les enregistrements A/AAAA et CNAME) seront analysés et utilisés pour enrichir l'inventaire dans les pipelines Cisco Secure Workload (comme appartenant au détenteur sous lequel l'orchestrateur est configuré) avec une seule étiquette à valeurs multiples appelée « orchestrator_system/dns_name », dont la valeur correspond aux entrées DNS qui pointent (directement ou indirectement) vers cette adresse IP.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité

- Serveurs DNS pris en charge : BIND9, serveurs prenant en charge AXFR (RFC 5936), Microsoft Windows Server 2016

Champs de configuration

- **Les zones DNS** sont un tableau de chaînes, dont chacune représente une zone DNS à transférer à partir du serveur DNS. Toutes les zones DNS doivent être précédées d'un point (« . »).
- **La liste d'hôtes** est un tableau de paires de noms d'hôte/adresse IP et de paires de ports pointant vers le ou les serveurs DNS à partir duquel récupérer les enregistrements DNS. Plusieurs serveurs DNS peuvent être configurés ici à des fins de haute disponibilité uniquement. Le comportement de haute disponibilité sur plusieurs serveurs DNS spécifiés dans hosts_list est celui de « premier serveur intègre » et favorisera les entrées les plus anciennes de hosts_list. Les zones ne peuvent pas être fractionnées sur les serveurs DNS.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur DNS est accessible sur cette adresse IP/ce port à partir de la grappe Cisco Secure Workload.
- Pour le TaaS ou dans les cas où le serveur DNS n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Configurez correctement les ACL/la configuration des transferts de zone DNS sur le serveur DNS. Reportez-vous à la documentation du logiciel de serveur DNS correspondant pour obtenir de plus amples renseignements.

Étiquettes générées

orchestrator_system/dns_name -> un champ à valeurs multiples dont les valeurs sont tous les noms d'hôte CNAME et A/AAAA pointant vers cette adresse IP.

Mises en garde

- Le flux de l'orchestrateur DNS est un *flux de métadonnées* : les adresses IP apprises lors d'un transfert de zone DNS ne créeront pas d'éléments d'inventaire dans Cisco Secure Workload. Au contraire, les étiquettes d'une adresse IP existante seront mises à jour avec les nouvelles métadonnées DNS. Les données DNS des adresses IP inconnues sont rejetées en mode silencieux. Afin d'annoter les métadonnées DNS des IP qui n'ont pas été apprises par un capteur ou via d'autres intégrations d'orchestrateur, les adresses IP doivent être téléversées via le mécanisme de téléversement en bloc de la CMDB afin de créer des entrées d'inventaire pour ces adresses. Les sous-réseaux appris des téléchargements CMDB ne créent pas d'entrées d'inventaire.
- Seuls les enregistrements CNAME et A/AAAA du serveur DNS sont traités. Les enregistrements CNAME seront transformés en enregistrements IPv4/IPv6 finaux via les enregistrements A/AAAA vers lesquels ils pointent. Un seul niveau de déférencement est pris en charge (c.-à-d. les chaînes CNAME -> CNAME -> A/AAAA ou plus ne sont pas déférencées) tant que CNAME pointe vers un enregistrement A/AAAA du même orchestrateur. Le déférencement CNAME sur différents orchestrateurs DNS n'est pas pris en charge.

Dépannage

- Problèmes de connexion

  Cisco Secure Workload tentera de se connecter au nom d'adresse IP/nom d'hôte et au numéro de port fournis en utilisant une connexion TCP provenant de l'un des serveurs d'appareils Cisco Secure Workload, du nuage dans le cas de TaaS, ou de la machine virtuelle hébergeant le service de tunnel VPN de connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic.

- Problèmes de privilège DNS AXFR

  De plus, la plupart des serveurs DNS (BIND9 ou Windows DNS ou Infoblox) nécessitent une configuration supplémentaire lorsque les adresses IP des clients tentent des transferts de zone DNS (requêtes AXFR selon les codes d'opération du protocole DNS), car ceux-ci sont plus exigeants en ressources et privilégiés que de simples requêtes DNS pour résoudre des enregistrements DNS individuels. Ces erreurs s'affichent généralement comme un refus AXFR, avec le code de raison 5 (REFUSÉ).

  Ainsi, tout test manuel visant à établir que le serveur DNS est configuré correctement ne doit pas dépendre de recherches réussies de nom d'hôte, mais doit plutôt tester spécifiquement les requêtes AXFR (à l'aide d'un outil comme dig).

  Tout échec lors d'un transfert de zone AXFR à partir du serveur DNS sera signalé dans le champ « authentication_failure_error » par l'appareil Cisco Secure Workload.

  En outre, notez que Cisco Secure Workload tentera des transferts de zone à partir de toutes les zones DNS configurées et que toutes doivent réussir pour que les données DNS soient insérées dans la base de données d'étiquettes Cisco Secure Workload.

- Les champs de nom d'hôte de l'inventaire ne sont pas remplis par DNS. Le « nom d'hôte » est toujours appris à partir du capteur Cisco Secure Workload. Si l'inventaire a été téléversé par le téléchargement dans la CMDB et non à partir du capteur, il manque peut-être le nom d'hôte. Toutes les données du flux de travail de l'orchestrateur DNS ne s'affichent que sous l'étiquette « orchestrator_system/dns_name » et ne rempliront jamais le champ du nom d'hôte.

Comportement de l'interrogation complète/additionnelle pour les orchestrateurs DNS

L'intervalle par défaut des instantanés complets est de 24 heures

L'intervalle par défaut des instantanés différentiels est de 60 minutes

Il s'agit également des valeurs minimales autorisées pour ces minuteurs.

Les enregistrements DNS ne changent que rarement. Ainsi, pour un comportement de récupération optimale, à chaque intervalle d'instantané différentiel, Cisco Secure Workload vérifie si les numéros de série de l'une des zones DNS ont été modifiés par rapport à l'intervalle précédent. Si aucune zone n'a changé, aucune action n'est nécessaire.

Si des zones ont été modifiées, nous effectuerons un transfert de zone à partir de toutes les zones DNS configurées (pas seulement de la zone qui a été modifiée).

À chaque intervalle d'instantané complet, les transferts de zone sont téléchargés à partir de toutes les zones et injectés par Cisco Secure Workload dans la base de données des étiquettes, que les numéros de série des zones aient changé ou non.

Fonctionnalités non prises en charge

Warning

- Les alias et les recherches DNAME ne sont pas pris en charge.
- Les transferts de zone incrémentiels (IXFR) ne sont pas pris en charge.

Infoblox

L'intégration Infoblox permet à Cisco Secure Workload d'importer des sous-réseaux Infoblox, des hôtes (*Record:host*) et des enregistrements A/AAAA dans la base de données d'inventaire de Cisco Secure Workload. Les noms et les valeurs des attributs extensibles sont importés tels quels et peuvent être utilisés comme étiquettes Cisco Secure Workload pour définir la portée et les politiques d'application.

Note Seuls les objets Infoblox avec des attributs extensibles sont pris en compte, c.-à-d. ceux auxquels aucun attribut extensible n'est attaché seront exclus de l'importation.

L'image ci-dessous montre un exemple d'étiquettes générées pour un objet hôte importé d'Infoblox avec l'attribut extensible *Department* :

Figure 14: Exemples d'étiquettes Infoblox

```
1. orchestrator_Department = AES789
2. orchestrator_system/cluster_id = [redacted]
3. orchestrator_system/cluster_name = scale13-ib
4. orchestrator_system/machine_id =
   record:host/[redacted]:client8/%20
5. orchestrator_system/machine_name = client8
6. orchestrator_system/orch_type = infoblox
```

Prérequis

- Point terminal d'API REST Infoblox prenant en charge WAPI version 2.6, 2.6.1, 2.7 et 2.7.1 (recommandé)

Champs de configuration

En plus des champs de configuration courants, décrits dans la section *Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Liste d'hôtes	Oui	La liste des hôtes indique une grille Infoblox, c'est-à-dire que plusieurs membres de la grille avec accès à l'API REST peuvent être ajoutés, et l'orchestrateur externe passera à la grille suivante dans la liste en cas d'erreurs de connexion. Si vous souhaitez importer des étiquettes d'une autre grille Infoblox, créez un nouvel orchestrateur externe pour celle-ci.

Note Pour les orchestrateurs externes Infoblox, les adresses IPv4 et IPv6 (mode pile double) sont prises en charge. Cependant, notez que la prise en charge de la double pile est une fonctionnalité bêta.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST Infoblox est accessible à partir de la grappe Cisco Secure Workload.
- Dans l cas du TaaS ou lorsque le serveur Infoblox n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Créez un orchestrateur externe de type *Infoblox*. Selon le volume des données Infoblox, c'est-à-dire le nombre de sous-réseaux, d'hôtes et d'enregistrements A/AAAA, il peut s'écouler jusqu'à une heure avant que le premier instantané complet soit disponible dans Cisco Secure Workload.
- Lors de la création de la configuration Infoblox, l'utilisateur a la possibilité de désélectionner n'importe quel type d'enregistrement (sous-réseau, hôte, enregistrements A/AAAA).

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes à tous les objets extraits d'Infoblox.

Clé	Valeur
orchestrator_system/orch_type	infoblox
orchestrator_system/cluster_id	UUID de l'orchestrateur externe dans Cisco Secure Workload
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/machine_id	<Référence/identifiant de l'objet Infoblox>
orchestrator_system/machine_name	<nom de l'hôte Infoblox (DNS)>

Étiquettes générées

Tous les attributs extensibles Infoblox seront importés en tant qu'étiquettes Cisco Secure Workload avec le préfixe *orchestrator_*. Par exemple, un hôte avec un attribut extensible appelé *Department* (service) peut être appelé dans la recherche d'inventaire Cisco Secure Workload en tant que *service_orchestrateur*.

Clé	Valeur
orchestrator_<extensible attribute>	<valeur(s) de l'attribut extensible telle(s) qu'extraite(s) d'Infoblox>

Mises en garde

- Le nombre maximal de sous-réseaux pouvant être importés à partir d'Infoblox est de 50 000.
- Le nombre maximal d'hôtes et d'enregistrements A/AAAA qui peuvent être importés à partir d'Infoblox est de 400 000 au total.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de TaaS , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez des privilèges pour envoyer des demandes d'API REST à l'appareil Infoblox.
- Tous les objets attendus ne sont pas importés. Cisco Secure Workload importe uniquement des sous-réseaux, des hôtes et des enregistrements A/AAAA auxquels des attributs extensibles sont attachés. Notez qu'il y a une limite au nombre d'objets qui peuvent être importés d'Infoblox, consultez *Mises en garde*.
- Impossible de trouver des sous-réseaux dans l'inventaire. Il n'est pas possible d'utiliser la recherche dans l'inventaire pour trouver des sous-réseaux Infoblox car l'inventaire Cisco Secure Workload par conception ne comporte que des adresses IP, c'est-à-dire des hôtes et des enregistrements A/AAA.
- Impossible de trouver un hôte ou un enregistrement A/AAAA, Cisco Secure Workload importe tous les attributs extensibles tels qu'ils ont été récupérés d'Infoblox. N'oubliez pas d'ajouter le préfixe *orchestrator_* au nom de l'attribut extensible, dans p. ex. la recherche d'inventaire. Notez que les attributs extensibles des sous-réseaux, s'ils ne sont pas marqués comme hérités dans Infoblox, ne font pas partie des hôtes et ne peuvent donc pas être recherchés dans Cisco Secure Workload.

F5 BIG-IP

L'intégration F5 BIG-IP permet à Cisco Secure Workload d'importer les *serveurs virtuels* à partir d'un dispositif d'équilibreur de charge F5 BIG-IP et d'en dériver des inventaires de services. Un inventaire de service correspond à un serveur virtuel F5 BIG-IP, dont le service se caractérise par la *VIP* (adresse IP virtuelle), le protocole et le port. Une fois importé dans Cisco Secure Workload, cet inventaire de service aura des

étiquettes telles que *service_name*, qui peuvent être utilisées dans la recherche d'inventaire ainsi que pour créer des portées et des politiques Cisco Secure Workload.

Un des gros avantages de cette fonctionnalité est l'application des politiques, car l' *orchestrateur externe pour F5 BIG-IP* traduit les politiques Cisco Secure Workload en règles de sécurité attribuées au serveur virtuel et les déploie sur l'équilibreur de charge F5 BIG-IP au moyen de son API REST.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Point de terminaison d'API REST F5 BIG-IP, version 12.1.1

Champs de configuration

En plus des champs de configuration courants, décrits dans la section *Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champ	Obligatoire	Description
Liste d'hôtes	Oui	Ceci spécifie le point de terminaison de l'API REST pour l'équilibreur de charge F5 BIG-IP. Si la haute disponibilité est configurée pour F5 BIG-IP, saisissez le nœud membre de secours de sorte qu'en cas de basculement, l'orchestrateur externe bascule sur le nœud actuel. Si vous souhaitez importer des étiquettes d'un autre équilibreur de charge F5 BIG-IP, vous devez créer un nouvel orchestrateur externe.
Activer l'application	Non	La valeur par défaut est faux (non cochée). Si cette option est cochée, cette option permet à Cisco Secure Workload *l'application des politiques* afin de déployer les règles de politique de sécurité sur l'équilibreur de charge F5 BIG-IP correspondant. Notez que les renseignements d'authentification fournis doivent avoir un accès en écriture sur l'API REST F5 BIG-IP.

Champ	Obligatoire	Description
Domaine de routage	Non	La valeur par défaut est 0 (zéro). Le domaine de routage spécifie quels serveurs virtuels doivent être pris en compte par l'orchestrateur externe. Le nombre est déterminé par la liste des partitions affectées à un domaine de routage donné, et seuls les serveurs virtuels définis dans ces partitions seront importés dans Cisco Secure Workload.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST F5 BIG-IP est accessible à partir de Cisco Secure Workload.
- Pour le TaaS ou dans les cas où l'appareil F5 BIG-IP n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour assurer la connectivité.
- Créez un orchestrateur externe de type *F5 BIG-IP*.
- Selon la valeur de l' *intervalle*, le premier instantané complet des serveurs virtuels F5 BIG-IP peut prendre jusqu'à 60 secondes (intervalle par défaut). Par la suite, les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes pour un orchestrateur externe pour *F5 BIG-IP* :

Clé	Valeur
orchestrator_system/orch_type	F5
orchestrator_system/cluster_id	<UUID de l'orchestrateur externe>
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/workload_type	service
orchestrator_system/namespace	<Partition à laquelle appartient le serveur virtuel>
orchestrator_system/service_name	<Nom du serveur virtuel F5 BIG-IP>

Étiquettes générées

Pour chaque serveur virtuel, l'orchestrateur externe génère les étiquettes suivantes :

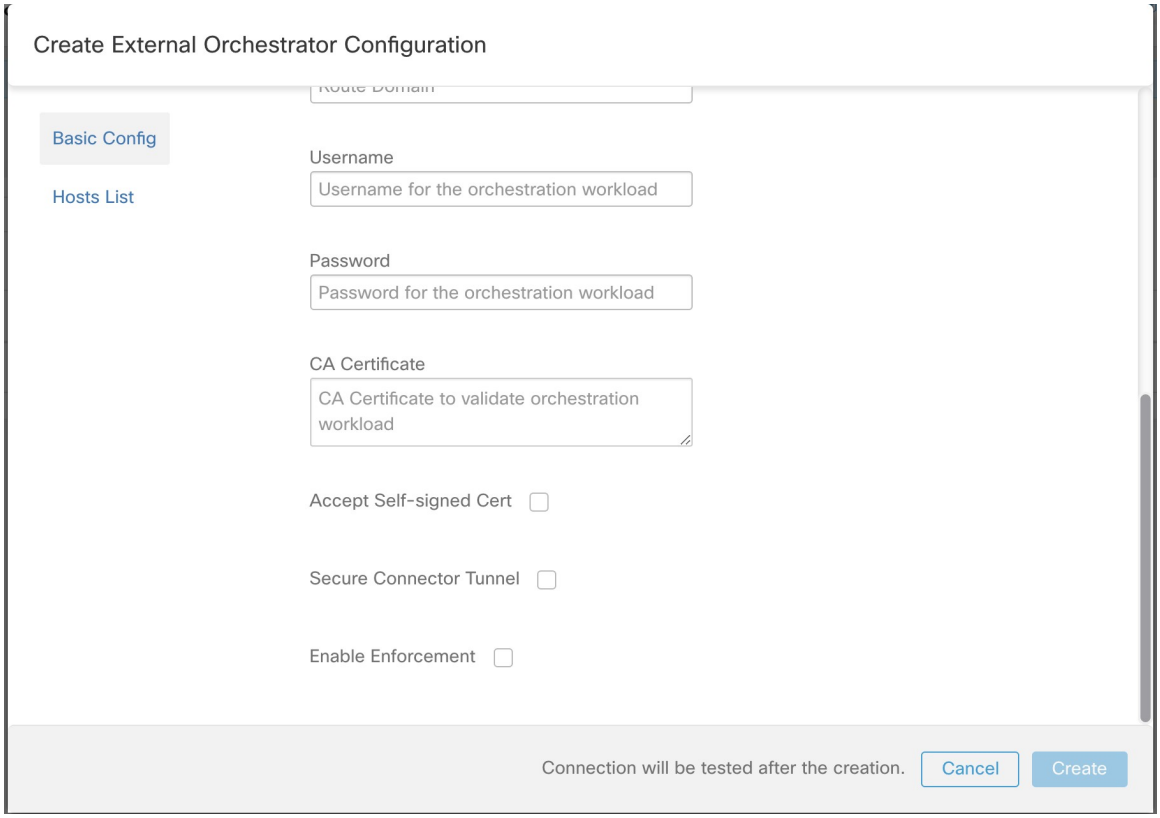
Clé	Valeur
orchestrator_annotation/snat_address	<Adresse SNAT des serveurs virtuels>

Application de la politique pour F5 BIG-IP

Cette fonctionnalité permet à Cisco Secure Workload de traduire les politiques logiques par des groupes de fournisseurs qui correspondent aux serveurs virtuels étiquetés *F5 BIG-IP* en règles de sécurité *F5 BIG-IP* et de les déployer sur le dispositif de l'équilibreur de charge à l'aide de son API REST. Comme mentionné ci-dessus, toute affectation de politique de sécurité existante au serveur virtuel *F5 BIG-IP* respectif sera remplacée par une nouvelle affectation pointant vers la politique de sécurité générée Cisco Secure Workload. Les politiques de sécurité existantes ne seront pas modifiées ni supprimées de la liste des politiques *F5 BIG-IP*.

Par défaut, l'application n'est pas activée dans la configuration de l'orchestrateur externe :

Figure 15: Option de configuration « Enable Enforcement » (Activer l'application)

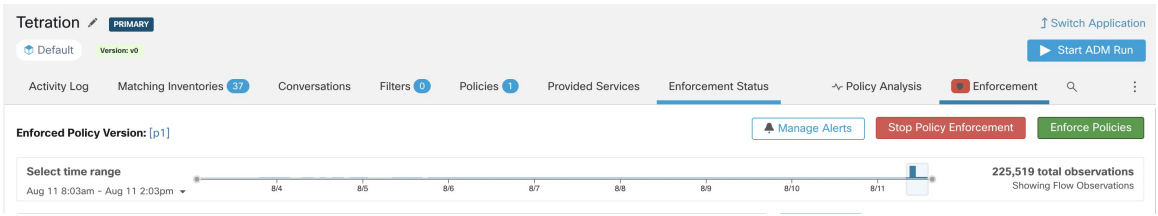


Cette option peut être modifiée à tout moment au besoin.

L'activation de l'application ne déploie pas les politiques sur l'équilibreur de charge tant que l'application n'est pas activée dans un espace de travail comprenant au moins une politique applicable à l'équilibreur de charge, ou suite à des mises à jour d'inventaires.

Cependant, la désactivation de l'application pour l'orchestrateur entraînera la suppression immédiate de toutes les règles de politique de sécurité déployées de l'équilibreur de charge *F5 BIG-IP*.

Figure 16: Application des politiques de l'espace de travail



Note

- L'orchestrateur pour *F5 BIG-IP* détecte également tout écart des règles de politique de sécurité et le remplace par des politiques Cisco Secure Workload. Toute modification de politique envers les serveurs virtuels doit être effectuée qu'avec Cisco Secure Workload.
- Lorsque l'application de la politique est arrêtée ou que l'orchestrateur externe est supprimé, la politique de sécurité des serveurs virtuels deviendra vide, car toutes les politiques Cisco Secure Workload seront supprimées de l'équilibreur de charge *F5 BIG-IP*.

L'état d'application de la politique OpenAPI pour l'orchestrateur externe peut être utilisé pour récupérer l'état de l'application de la politique Cisco Secure Workload sur le dispositif de l'équilibreur de charge associé à l'orchestrateur externe. Cela permet de vérifier si le déploiement des règles de politique de sécurité sur l'appareil *F5 BIG-IP* a réussi ou échoué.

Application des politiques au contrôleur d'entrée F5

Cisco Secure Workload applique les politiques à la fois au niveau de l'équilibreur de charge *F5 BIG-IP* et au niveau des pods du backend lorsque les pods sont accessibles aux clients externes à l'aide de l'objet d'entrée de Kubernetes.

Voici les étapes à suivre pour appliquer la politique à l'aide du contrôleur d'entrée F5.

Procedure

Étape 1 Créez un orchestrateur externe pour l'équilibreur de charge *F5 BIG-IP* , comme décrit précédemment.

Étape 2 Créez un orchestrateur externe pour Kubernetes/OpenShift comme décrit ici.

```
→  ~
→  ~ k8s get ingress
NAME           HOSTS   ADDRESS          PORTS   AGE
test-ingress   *       192.168.60.100   80      7s
→  ~
```

Étape 3 Créez un objet d'entrée dans la grappe Kubernetes. Un instantané du fichier yaml utilisé pour créer l'objet d'entrée est fourni dans l'image suivante.

```
→  ~
→  ~ k8s get ingress test-ingress -o yaml
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  annotations:
    virtual-server.f5.com/ip: 192.168.60.100
    virtual-server.f5.com/partition: k8scluster
  creationTimestamp: "2019-07-26T18:34:39Z"
  generation: 1
  name: test-ingress
  namespace: default
  resourceVersion: "8310"
  selfLink: /apis/extensions/v1beta1/namespaces/default/ingresses/test-ingress
  uid: 06f8a705-afd4-11e9-97fb-525400d58002
spec:
  backend:
    serviceName: nginx
    servicePort: 80
status:
  loadBalancer:
    ingress:
    - ip: 192.168.60.100
→  ~
```

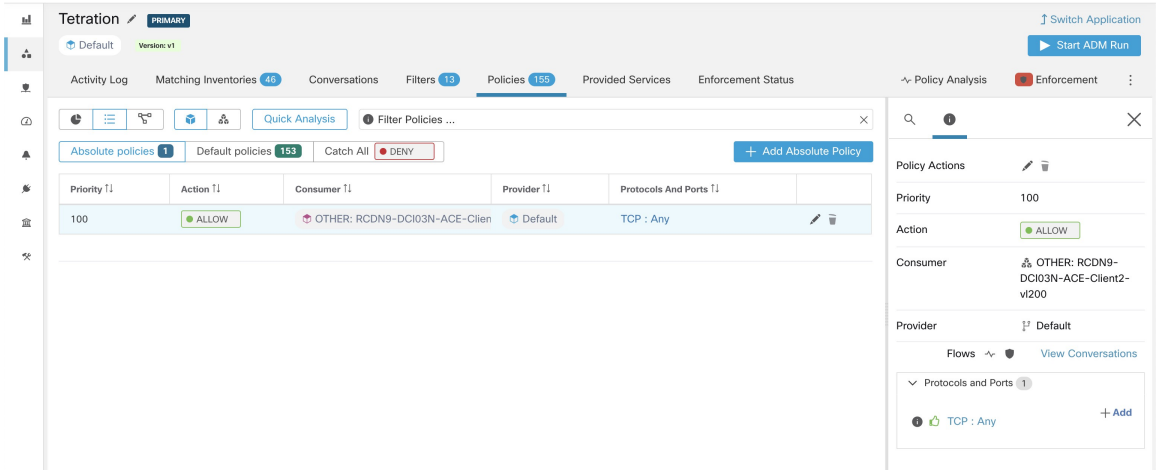
Étape 4 Déployez un pod de contrôleur d'entrée F5 dans la grappe Kubernetes.

```
→  ~ k8s get deploy -n kube-system
NAME                    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
coredns                 2         2         2            2           31m
k8s-bigip-ctlr-cluster  1         1         1            1           5m20s
→  ~
```

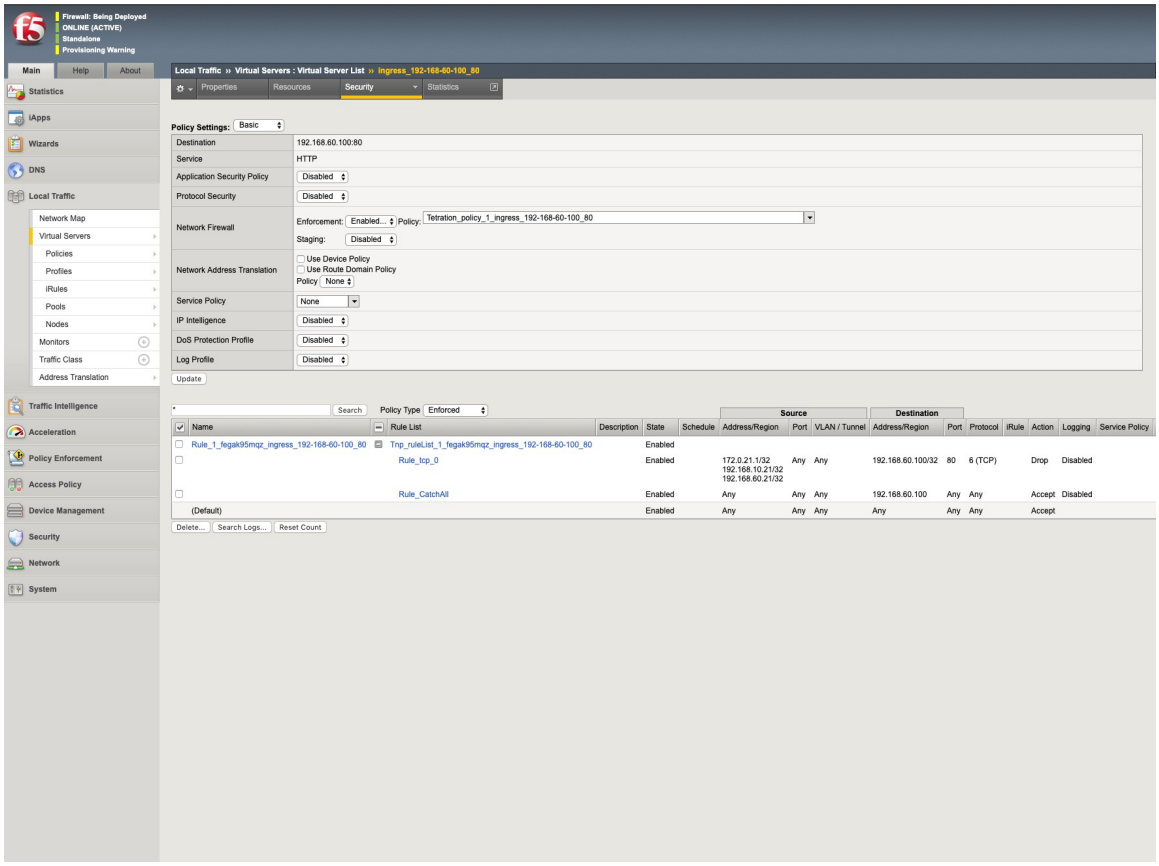
Étape 5 Créez un service de serveur backend (principal) auquel les consommateurs externes à la grappe accèdent. Dans l'exemple ci-dessous, nous avons créé un service *nginx* .

```
→  ~
→  ~ k8s get deploy
NAME    DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
nginx   1         1         1            0           5s
→  ~
```

Étape 6 Créez une politique entre le consommateur externe et le service backend. Appliquez la politique à l'aide de l'onglet *Policy Enforcement* (Application des politiques).



Étape 7 Vérifiez les politiques sur l'équilibreur de charge *F5 BIG-IP* et les pods du backend. Dans le cas de F5, l'équilibreur de charge Cisco Secure Workload appliquera la règle d'autorisation/abandon appropriée où la source sera le consommateur spécifié à l'étape 6 et la destination sera la VIP [VIP du service virtuel Ingress pour F5]. Dans le cas de pods du serveur principal (backend), Cisco Secure Workload appliquera la règle autoriser/abandonner appropriée où la source sera le SNIP [dans le cas où le pool SNAT est activé] ou l'IP F5 [carte automatique activée] et la destination sera l'adresse IP du pod de backend.



Mises en garde

- Pendant la phase de déploiement du mode *F5 BIG-IP* HA, activez l'option *de synchronisation de la configuration* . Cela garantit que l'orchestrateur externe peut récupérer la dernière liste de serveurs virtuels auprès de l'hôte actuellement connecté.
- Dans le cas d'un mode de déploiement *F5 BIG-IP* HA, si la mise en correspondance *automatique* est configurée au lieu du regroupement SNAT pour la traduction d'adresses, assurez-vous que l'*adresse IP BIG-IP principale* est configurée avec l'adresse *Self IP* (Auto IP) flottante.
- Seule l'adresse VIP définie comme une adresse unique est prise en charge. L'adresse VIP donnée comme sous-réseau n'est pas prise en charge.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de *TaaS* , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez de privilèges d'accès en lecture et en écriture pour envoyer des requêtes d'API REST à l'appareil *F5 BIG-IP*.
- Règles de sécurité introuvables : Si aucune règle de sécurité n'est trouvée pour un serveur virtuel défini, après l'application de la politique, assurez-vous que le serveur virtuel correspondant est activé, c.-à-d. sa disponibilité/état doit être *disponible*/*activé*.

Citrix Netscaler

L'intégration Citrix Netscaler permet à Cisco Secure Workload d'importer les *serveurs virtuels d'équilibrage de la charge* à partir d'un dispositif d'équilibreur de charge Netscaler et d'en dériver des inventaires de services. Un inventaire de service correspond à un service Netscaler fourni par un serveur virtuel et possède des étiquettes telles que *service_name* (nom_service), qui peuvent être utilisées dans la recherche d'inventaire et pour créer des portées et des politiques pour Cisco Secure Workload.

Un des principaux avantages de cette fonctionnalité est l'application des politiques, car l'*orchestrateur externe pour Citrix Netscaler* traduit les politiques Cisco Secure Workload en règles de liste de contrôle d'accès Netscaler et les déploie sur l'équilibreur de charge Netscaler via son API REST.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Point terminal de l'API REST Netscaler version 12.0.57.19

Champs de configuration

En plus des champs de configuration courants, décrits dans la section *Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Liste d'hôtes	Oui	Ceci spécifie le point terminal de l'API REST pour l'équilibreur de charge Citrix Netscaler. Si la haute disponibilité est configurée sur Citrix Netscaler, saisissez un autre nœud membre de sorte qu'en cas de basculement, l'orchestrateur externe bascule sur le nœud actuel. Si vous souhaitez importer des étiquettes d'un autre équilibreur de charge Citrix Netscaler, créez un nouvel orchestrateur externe.
Activer l'application	Non	La valeur par défaut est faux (non cochée). Si cette option est cochée, cela permet Cisco Secure Workload *à l'application de la politique* de déployer les règles ACL sur l'équilibreur de charge Citrix Netscaler correspondant. Notez que les informations d'authentification fournies doivent autoriser un accès en écriture à l'API REST Citrix Netscaler.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le point terminal de l'API REST Netscaler est accessible à partir de la grappe Cisco Secure Workload.
- Pour le TaaS ou dans les cas où l'appareil Netscaler n'est pas accessible directement, l'utilisateur doit configurer un tunnel de connecteur sécurisé pour fournir la connectivité.
- Créez un orchestrateur externe avec le type *Citrix Netscaler*.
- Selon la valeur de l'*intervalle*, cela peut prendre jusqu'à 60 secondes (intervalle par défaut) avant que le premier instantané complet des serveurs virtuels Netscaler ne se termine. Par la suite, les étiquettes générées peuvent être utilisées pour créer des portées et des politiques d'application Cisco Secure Workload.
- Appliquer les politiques de Cisco Secure Workload pour déployer les règles d'ACL Netscaler.

Étiquettes générées par l'orchestrateur

Cisco Secure Workload ajoute les étiquettes système suivantes pour un orchestrateur externe pour *Citrix Netscaler* :

Clé	Valeur
orchestrator_system/orch_type	nsbalancer
orchestrator_system/cluster_id	<UUID de l'orchestrateur externe>
orchestrator_system/cluster_name	<Nom donné à cet orchestrateur externe>
orchestrator_system/workload_type	service
orchestrator_system/service_name	<Nom du serveur virtuel d'équilibrage de charge>

Étiquettes générées

Pour chaque serveur virtuel d'équilibrage de charge, l'orchestrateur externe génère les étiquettes suivantes :

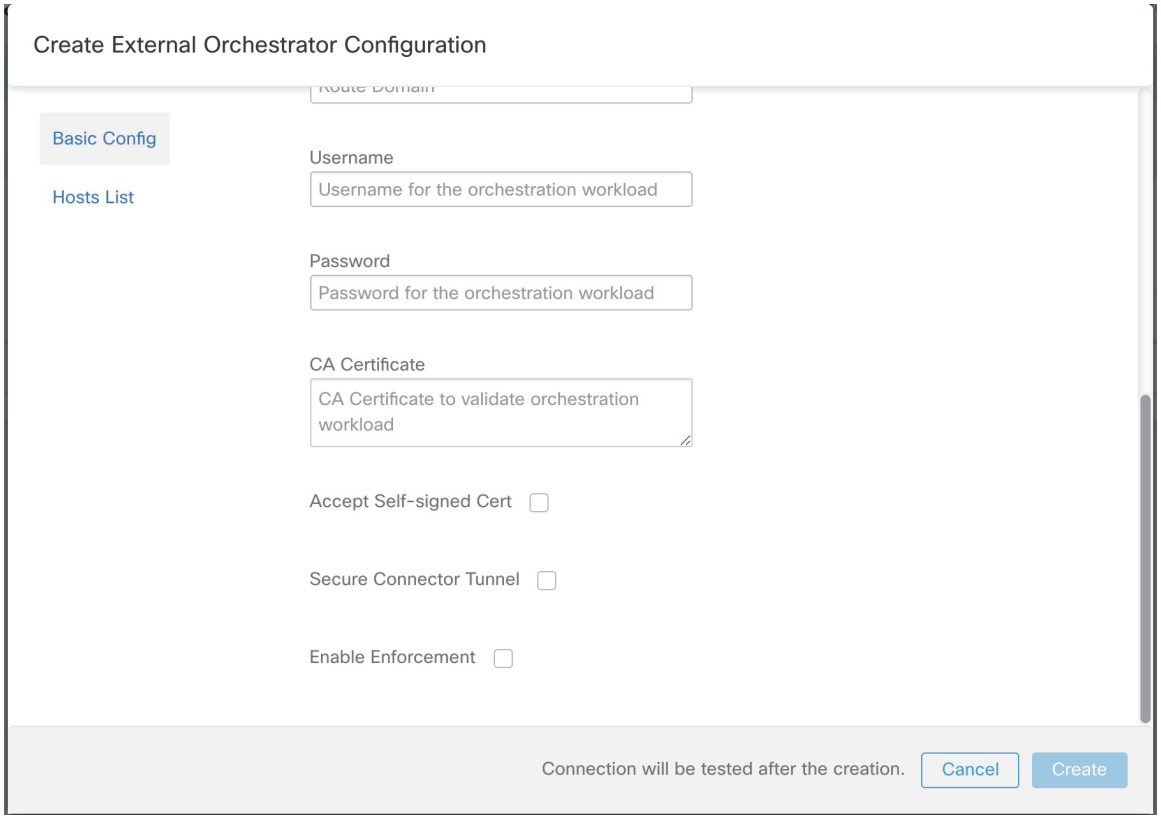
Clé	Valeur
orchestrator_annotation/snat_address	<Adresse SNAT des serveurs virtuels>

Application de la politique pour Citrix Netscaler

Cette fonctionnalité permet à Cisco Secure Workload de traduire les politiques logiques avec des groupes de fournisseurs qui correspondent aux serveurs virtuels étiquetés *Citrix Netscaler* en règles ACL *Citrix Netscaler* et de les déployer sur le dispositif de l'équilibreur de charge à l'aide de son API REST. Comme mentionné ci-dessus, toutes les règles ACL existantes seront remplacées par des règles de politique générées par Cisco Secure Workload.

Par défaut, le champ *Enable Enforcement* (Activer l'application) n'est pas coché. c'est à dire est désactivé, dans la boîte de dialogue *Create Orchestrator* (Créer un orchestrateur), comme le montre l'image ci-dessous :

Figure 17: Option de configuration « Enable Enforcement » (Activer l'application)



Il suffit de cocher la case désignée pour activer l'application pour l'orchestrateur. Cette option peut être modifiée à tout moment au besoin.

Activer l'application pour l'orchestrateur, que cela se fasse en créant ou en modifiant la configuration de l'orchestrateur, ne déploiera pas immédiatement les politiques logiques actuelles sur le dispositif de l'équilibreur de charge. Cette tâche est effectuée dans le cadre de l'application de la politique d'espace de travail qui doit être déclenchée par l'utilisateur, comme le montre l'image suivante, ou en raison d'une mise à jour des inventaires. Cependant, la désactivation de l'application pour l'orchestrateur entraînera la suppression immédiate de toutes les règles ACL déployées de l'équilibreur de charge *Citrix Netscaler*.

Figure 18: Application des politiques de l'espace de travail

Note

- L'orchestrateur pour *Citrix Netscaler* détecte également tout écart par rapport aux règles ACL et le remplace par des politiques Cisco Secure Workload. Toute modification de politique à l'égard des serveurs virtuels d'équilibrage de charge doit être effectuée avec Cisco Secure Workload uniquement.
- Lorsque l'application des politiques est arrêtée ou que l'orchestrateur externe est supprimé, les listes de contrôle d'accès (ACL) deviennent vides, car toutes les politiques Cisco Secure Workload sont supprimées de l'équilibreur de charge *Citrix Netscaler*.

L'état d'application de la politique OpenAPI pour l'orchestrateur externe peut être utilisé pour récupérer l'état de l'application de la politique Cisco Secure Workload sur le dispositif de l'équilibreur de charge associé à l'orchestrateur externe. Cela permet de vérifier si le déploiement des règles ACL sur l'appareil *Citrix Netscaler* a réussi ou échoué.

Mises en garde

- Si l'application est activée, les politiques Cisco Secure Workload seront toujours déployées sur la liste globale des ACL, c.-à-d. *par défaut* de la partition.
- Seule l'adresse VIP définie comme une adresse unique est prise en charge. L'adresse VIP donnée comme modèle d'adresse n'est pas prise en charge.
- La visibilité des services détectés (serveurs virtuels *Citrix Netscaler*) n'est pas prise en charge.

Dépannage

- Problème de connectivité, Cisco Secure Workload tentera de se connecter à l'adresse IP/au nom d'hôte et au numéro de port fournis à l'aide d'une connexion HTTPS provenant de l'un des serveurs d'appareils Cisco Secure Workload ou du nuage dans le cas de *TaaS* , ou de la machine virtuelle hébergeant le service de tunnel de Connecteur sécurisé Cisco Secure Workload. Afin d'établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic. Assurez-vous également que les informations d'authentification fournies sont correctes et que vous disposez de privilèges d'accès en lecture et en écriture pour envoyer des requêtes d'API REST à l'appareil *Citrix Netscaler*.
- Règles ACL introuvables. Si aucune règle ACL n'est trouvée, après l'application de la politique, assurez-vous que le serveur virtuel correspondant est activé, c.-à-d. son état doit être *opérationnel*.

TAXII

L'intégration TAXII (Trusted Automated Exchange of Intelligence Information) permet à Cisco Secure Workload d'acquérir les flux de données de renseignements sur les menaces des fournisseurs de sécurité pour annoter les flux réseau et les condensés de processus à l'aide d'indicateurs STIX (Structured Threat Information Expression) comme les adresses IP malveillantes, les condensés malveillants.

Lorsqu'une configuration d'orchestrateur externe est ajoutée pour le type « taxii », l'appareil Cisco Secure Workload tente de se connecter au(x) serveur(s) TAXII et interroge les collections de flux de données STIX. Les flux de données STIX (uniquement les adresses IP et les indicateurs de condensé binaires) seront analysés

et utilisés pour annoter les flux réseau et les condensés de processus dans les pipelines de Cisco Secure Workload (comme appartenant au détenteur sous lequel l'orchestrateur est configuré).

Les flux réseau avec des adresses de fournisseur ou de consommateur correspondant à des adresses IP malveillantes importées seront étiquetés avec l'étiquette à valeurs multiples « orchestrator_malicious_ip_by_<nom du fournisseur> » où <nom du fournisseur> est l'entrée de configuration de l'orchestrateur d'utilisateur du fournisseur TAXII et la valeur de l'étiquette est « Yes » (Oui).

Les indicateurs de condensé binaire STIX intégrés seront utilisés pour annoter les condensés de processus de charge de travail, qui seront affichés (s'ils correspondent) dans le tableau de bord de sécurité et les détails de la note de condensé de processus, et dans le profil de charge de travail et condensés de fichier.

Prérequis

- Tunnel du connecteur sécurisé, si nécessaire pour la connectivité
- Serveurs TAXII pris en charge : 1.0
- Flux TAXII pris en charge avec la version STIX : 1.x

Champs de configuration

En plus des champs de configuration courants, décrits dans la section *Créer un orchestrateur externe*, les champs suivants peuvent être configurés :

Champs communs	Obligatoire	Description
Nom	Oui	Nom de l'orchestrateur spécifié par l'utilisateur.
Description	Oui	Description de l'orchestrateur précisée par l'utilisateur.
Fournisseur	Oui	Le fournisseur fournit les flux de données de renseignements.
Intervalle complet entre les instantanés	Oui	L'intervalle (en secondes) pour effectuer un instantané complet du flux TAXII. (Par défaut : 1 jour)
URL de l'interrogation	Oui	Le chemin d'accès complet de l'URL d'interrogation pour interroger les données.
Collecte	Oui	Le nom de la collecte de flux TAXII à interroger.
Jours d'interrogation	Oui	Le nombre de données sur les menaces de jours antérieurs à interroger à partir du flux TAXII.

Champs communs	Obligatoire	Description
Username		Nom d'utilisateur pour l'authentification.
Mot de passe		Mot de passe d'authentification.
Certificat		Votre certificat client servira à l'authentification.
Clé		Clé correspondant au certificat client.
Certificat de l'autorité de certification		Certificat de l'autorité de certification pour valider le point terminal de l'orchestration.
Accept Self-signed Cert (Accepter le certificat autosigné)		Case pour désactiver la vérification strictSSL du certificat du serveur TAXII API
Secure Connector Tunnel (Tunnel du connecteur sécurisé)		Connexions de tunnel vers les hôtes de cet orchestrateur par l'intermédiaire du tunnel du connecteur sécurisé.
Liste d'hôtes	Oui	Les paires nom d'hôte/adresse IP et la paire de ports pointant vers le ou les serveurs TAXII.

Flux de travaux

- Tout d'abord, l'utilisateur doit vérifier que le serveur TAXII est accessible sur cette adresse IP ou ce port à partir de la grappe Cisco Secure Workload.
- Configurez le serveur TAXII adéquat avec le chemin d'interrogation et le nom du flux TAXII.

Étiquettes générées

Clé	Valeur
orchestrator_system/orch_type	*TAXII*
orchestrator_system/cluster_id	L'identifiant unique UUID de la configuration de la grappe dans Cisco Secure Workload.
orchestrator_system/cluster_name	Nom donné à la configuration de cette grappe>.
orchestrator_malicious_ip_by_ <vendor>	*Yes (Oui)* , si l'adresse du fournisseur ou du client de flux correspond aux données d'adresses IP malveillantes TAXII importées.

Mises en garde

- L’intégration de TAXII est prise en charge uniquement sur Cisco Secure Workload sur site.
- Seuls les adresses IP et les indicateurs de condensé des flux TAXII font l'objet d'une intégration.
- Le nombre maximal d’adresses IP intégrées est de 100 K (dernière mise à jour) par flux TAXII.
- Le nombre maximal de condensés intégrés est de 500 K (dernière mise à jour) pour tous les flux TAXII.
- Seuls les flux TAXII avec STIX version 1.x sont pris en charge.

Dépannage

- Problèmes de connexion

  Le Cisco Secure Workload tentera de se connecter au chemin d’URL d’interrogation fourni à partir de l’un des Cisco Secure Workload serveurs d’appareils ou de la machine virtuelle qui héberge le service de tunnel VPN du connecteur sécuriséCisco Secure Workload. Afin d’établir correctement cette connexion, les pare-feu doivent être configurés pour autoriser ce trafic.

Comportement de l’interrogation complète pour les orchestrateurs TAXII

L’intervalle par défaut des instantanés complets est de 24 heures

À chaque intervalle d’instantané complet, Cisco Secure Workload extrait les flux TAXII des adresses IP et des condensés de fichiers jusqu’aux limites ci-dessus dans la base de données d’étiquettes.

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.