Configurer l'intégration du connecteur de charge de travail ISE avec VMware vCenter

Table des matières

- Introduction
- Conditions préalables
  - Exigences
    - Cisco ISE
    - VMware vCenter
    - Connectivité
    - Certificats
  - Composants utilisés
- Informations générales
  - Termes clés
  - Espaces réservés utilisés
- Configurer
  - Diagramme du réseau
  - Configurations
    - Étape 1. Ajout de la connexion de charge globale vCenter
    - Étape 2. Ajout d'attributs vCenter au dictionnaire (facultatif)
    - Étape 3. Classification des charges de travail en SGT
    - Étape 4. Liaisons de route avec les règles de domaine SGT entrantes et sortantes
- Vérifier
  - Vérification de l'état de la connexion
  - Vérification des groupes de sécurité
  - Vérification des liaisons IP-SGT
  - Vérification des sessions en direct de la charge globale
  - Vérification de la visibilité des charges de travail dans Context Visibility
- Dépannage
  - Problèmes courants
  - Activer les journaux de débogage
  - Alarmes
- Informations connexes

Introduction

Ce document décrit comment configurer Cisco ISE Workload Connector pour VMware vCenter pour importer le contexte de charge de travail/appliquer la segmentation basée sur les groupes.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de Cisco ISE
- Administration de VMware vCenter
- Les concepts Cisco TrustSec, notamment les balises SGT (Security Group Tags), SXP (SGT Exchange Protocol) et pxGrid

Avant d'ajouter une connexion de charge globale vCenter, vérifiez que ces conditions sont remplies.

Cisco ISE

- pxGrid est activé sur au moins un noeud du déploiement.
- SXP est activé sur au moins un noeud du déploiement.

VMware vCenter

- Un compte vCenter avec l'autorisation Lecture seule est disponible. Le connecteur effectue uniquement des opérations de lecture.
- Les attributs ou balises vCenter à importer ont été identifiés. Ce document utilise l'attribut os comme exemple.

Connectivité

- Une connexion Internet stable est disponible pour Cisco ISE, car Cisco ISE peut atteindre public.ecr.aws, ce qui est requis par la fonctionnalité Workload Connector. Si un serveur proxy ou un pare-feu se trouve sur le chemin, autorisez le trafic HTTPS (port TCP 443) entre Cisco ISE et cette URL. Si cette URL est inaccessible, le connecteur de charge globale ne fonctionne pas comme prévu.
- Si un proxy est utilisé pour l'accès à Internet et que vCenter est déployé sur site, configurez un contournement de proxy pour l'adresse IP vCenter.

Certificats

- Si la validation du certificat est utilisée, le nom de domaine complet ou l'adresse IP saisi pour vCenter doit correspondre au nom alternatif du sujet (SAN) du certificat du point d'extrémité vCenter.
- Le certificat racine vCenter doit être disponible pour l'importation dans le magasin de certificats de confiance Cisco ISE.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine (ISE), version 3.4, utilisé pour les procédures de configuration et de vérification des connecteurs
- Cisco Identity Services Engine (ISE), version 3.5 Patch 3, utilisé pour la procédure de visibilité du contexte uniquement
- VMware vCenter Server 8.0 Mise à jour 3



Remarque : Le tableau de bord Workload Connector Endpoints de Context Visibility requiert Cisco ISE 3.5 Patch 3 ou version ultérieure. Les deux images de cette section ont donc été capturées dans cette version. Toutes les autres procédures et images de ce document proviennent de Cisco ISE 3.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les data centers modernes sont dynamiques. Les machines virtuelles (VM) sont créées, déplacées et retirées en permanence, et leurs adresses IP changent avec elles. Les stratégies de sécurité qui reposent sur des adresses IP ou des sous-réseaux statiques ne peuvent pas suivre ce rythme de changement, ce qui laisse des lacunes dans l'application et la visibilité.

Cisco ISE résout ce problème grâce à la structure Common Policy Framework et à ses

connecteurs de charge de travail. Un connecteur de charge de travail établit une connexion sécurisée à un data center ou à une plate-forme cloud, importe le contexte des charges de travail d'application qui s'y exécutent, normalise ce contexte dans des balises SGT et partage le résultat avec le reste du réseau afin que la politique puisse être écrite en fonction de ce contexte.

vCenter décrit déjà chaque machine virtuelle à l'aide d'un ensemble d'attributs, tels que le système d'exploitation invité, le groupe de ports auquel elle est connectée et son état d'alimentation. Les administrateurs VMware complètent cette description par des balises personnalisées qui contiennent des métadonnées telles que l'environnement, le niveau application, le propriétaire ou l'unité commerciale. Le connecteur de charge de travail vCenter importe les deux et les convertit en balises SGT. Cela permet d'obtenir trois résultats :

- La politique est basée sur la charge de travail. Lorsqu'une VM est déplacée ou ré-adressée, le SGT dérivé des attributs reste avec elle, de sorte que la segmentation continue à fonctionner sans mises à jour manuelles.
- Le contexte existant est réutilisé. Cisco ISE utilise les attributs et les balises que vCenter gère déjà. Aucun nouveau schéma de classification n'est donc requis.
- La segmentation est cohérente. Les balises SGT sont distribuées sur le réseau compatible TrustSec, de sorte que la même stratégie s'applique à chaque point d'application.

Ce document utilise un seul exemple d'exécution. L'attribut de système d'exploitation que vCenter signale pour chaque machine virtuelle, qui, dans ces travaux pratiques, indique CentOS 4/5 (64 bits), est importé dans Cisco ISE et associé à une condition d'adresse IP, de sorte que les charges de travail correspondantes sont automatiquement placées dans un groupe de sécurité Production_Servers. Ces charges de travail sont ensuite segmentées par appartenance au groupe plutôt que par adresses IP suivies manuellement. La même procédure s'applique à tout autre attribut ou balise personnalisée exposé par vCenter.

Termes clés



Remarque : VMware ESXi ne prend pas en charge les balises. Pour cette raison, seul vCenter peut être configuré comme connecteur de charge de travail. Les hôtes ESXi autonomes ne le peuvent pas.

Terme	Définition
TrustSec	Technologie Cisco pour la segmentation par groupe, dans laquelle la politique est écrite en fonction des groupes plutôt qu'en fonction des adresses IP.

Terme	Définition
SGT (Security Group Tag)	Balise qui représente un groupe, tel que les charges de travail de production, et qui sert de base à l'application des stratégies.
SXP (SGT Exchange Protocol)	Protocole utilisé pour distribuer les liaisons IP à SGT aux périphériques d'application.
pxGrid	Plate-forme Cisco utilisée pour partager le contexte, par exemple les sessions et les balises de groupe de sécurité, entre Cisco ISE et d'autres systèmes.
politique commune	L'infrastructure Cisco ISE qui se connecte aux data centers et aux clouds, normalise leur contexte en SGT et le partage entre les domaines.
Connecteur de charge	Composant Cisco ISE qui se connecte à vCenter, AWS, Azure, GCP ou ACI et importe le contexte de charge de travail.

Espaces réservés utilisés

Les valeurs entre crochets sont des espaces réservés. Remplacez-les par les valeurs qui s'appliquent à votre environnement.

Espace réservé	Description
[VCENTER_FQDN]	Nom de domaine complet du serveur vCenter.
[ADRESSE_IP_VCENTER]	Adresse IP du serveur vCenter.
[NOM D'UTILISATEUR]	Nom d'utilisateur de compte en lecture seule vCenter.
[MOT DE PASSE]	Mot de passe de compte en lecture seule vCenter.
[NOM_SGT]	Nom de la balise du groupe de sécurité attribuée par une règle de classification.
[NOM_VM]	Nom d'une machine virtuelle dans vCenter.

Espace réservé	Description
[UUID_VM]	UUID d'une machine virtuelle dans vCenter.
[ID_VM]	Référence d'objet géré vCenter d'une machine virtuelle.
[ID_HÔTE]	Référence d'objet géré vCenter d'un hôte ESXi.
[NOM_RÉSEAU]	Nom du groupe de ports ou du réseau vCenter.

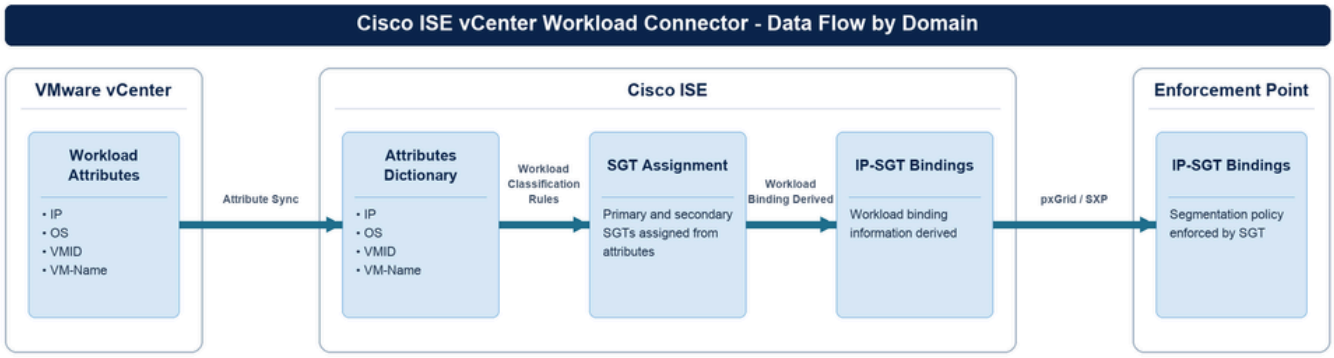
Les images de ce document proviennent d'un TP utilisant le nom de connexion de charge globale LAB_VCenter, l'adresse vCenter 192.168.1.50 et le sous-réseau de charge globale 192.168.10.0/24. Remplacez les noms et les adresses qui s'appliquent à votre environnement.

Configurer

Diagramme du réseau

L'intégration transforme les métadonnées vCenter en une politique applicable en cinq étapes :

1. Le connecteur de charge de travail Cisco ISE vCenter lit les attributs et les balises de charge de travail à partir de vCenter.
2. Les attributs sélectionnés sont ajoutés au dictionnaire d'attributs Cisco ISE afin qu'ils puissent être référencés dans les règles.
3. Les règles de classification de la charge globale évaluent ces attributs et attribuent un SGT principal, et éventuellement un ou plusieurs SGT secondaires, à chaque charge globale.
4. Cisco ISE dérive des liaisons IP à SGT et les publie via SXP et pxGrid. Les règles de domaine SGT entrantes et sortantes contrôlent quels domaines SGT reçoivent les liaisons et où elles sont partagées.
5. Les points d'application appliquent les balises SGT pour autoriser ou refuser le trafic.

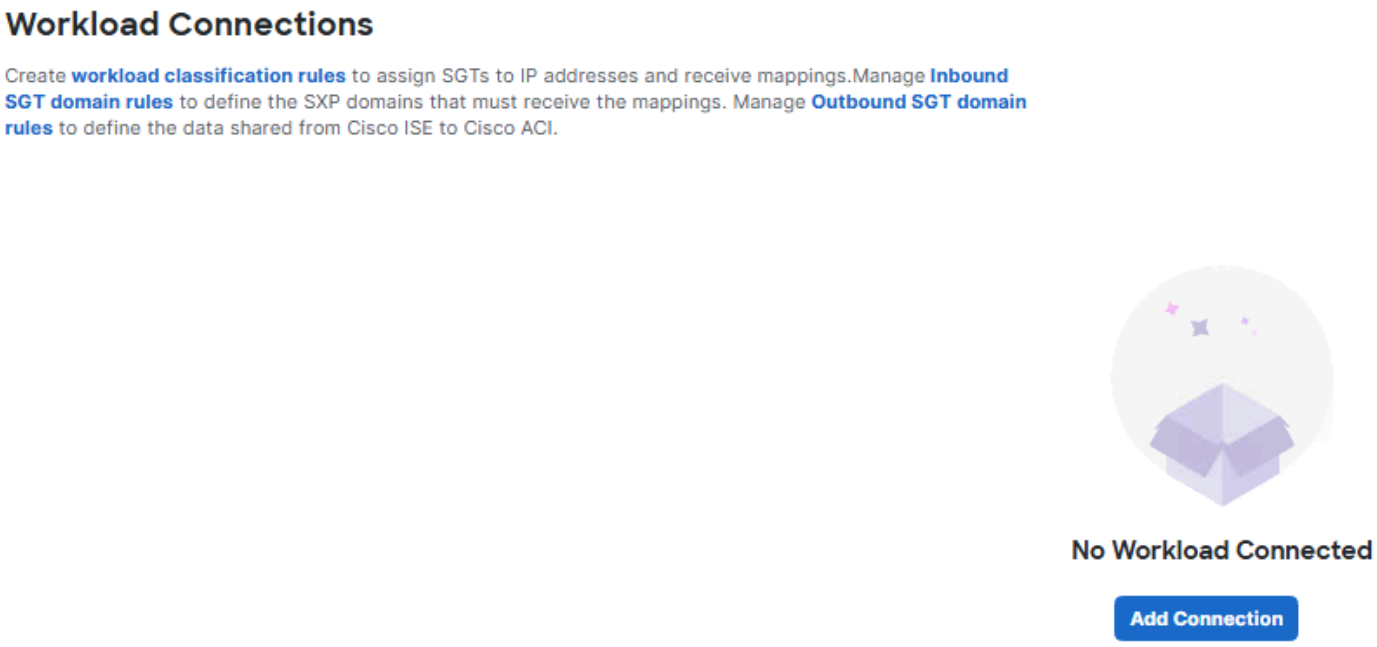


Le flux de données Cisco ISE vCenter Workload Connector s'étend sur trois domaines. vCenter fournit des attributs de charge de travail (IP, OS, VMID, VM-Name) ; Cisco ISE les stocke dans le dictionnaire d'attributs, applique des règles de classification de charge de travail pour attribuer des balises SGT principales et secondaires, et dérive des liaisons IP-SGT ; les liaisons sont partagées via pxGrid et SXP vers le point d'application

Configurations

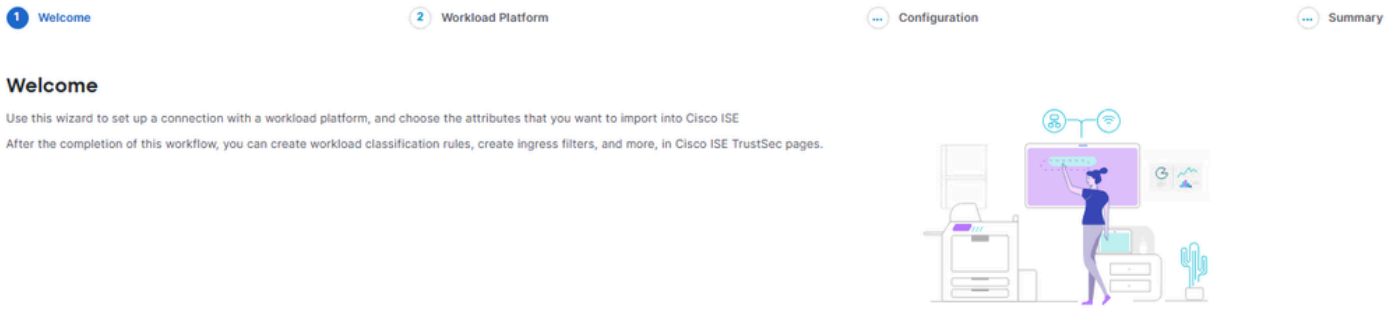
Étape 1. Ajout de la connexion de charge globale vCenter

1. Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur l'icône Menu et choisissez Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections.
2. Cliquez sur Ajouter une connexion.



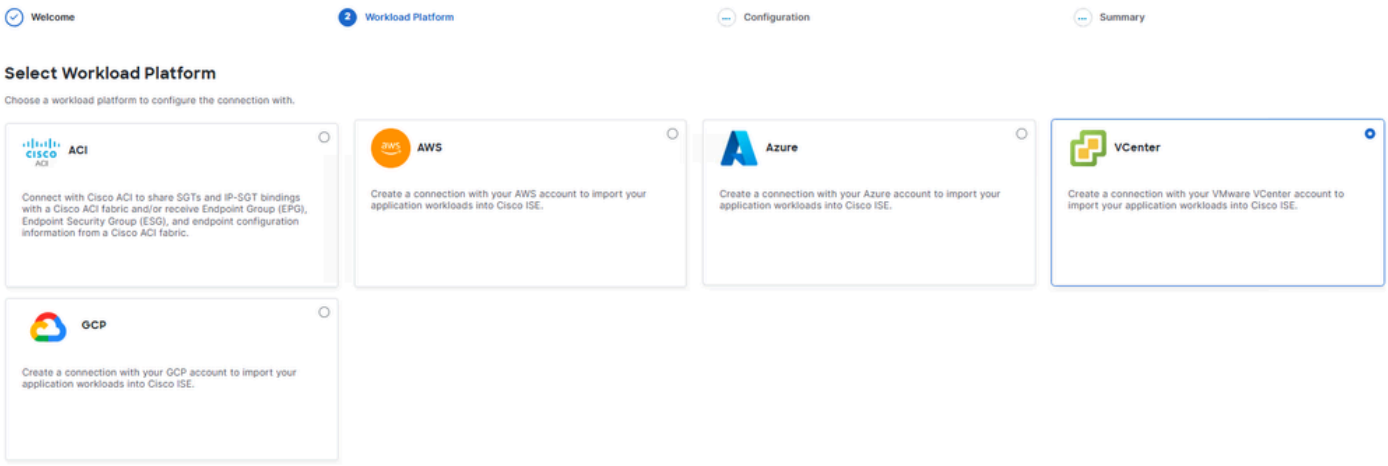
Page Connexions de charge globale sans connexion configurée, affichant le bouton Ajouter une connexion

3. Cliquez sur Let's do it.



Page d'accueil de l'assistant de connexion de charge globale, affichant les étapes Bienvenue, Plate-forme de charge globale, Configuration et Résumé de l'assistant

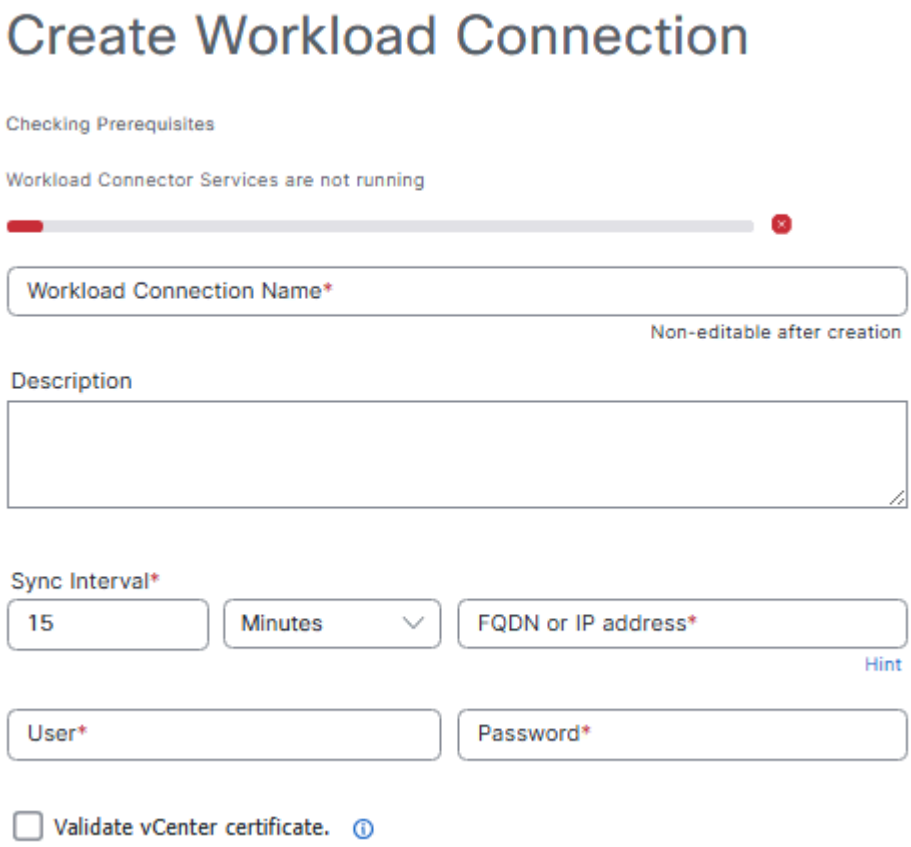
4. Sur la page Sélectionner une plate-forme de charge globale, choisissez vCenter, puis cliquez sur Suivant.



Sélectionnez la page Plate-forme de charge globale avec l'option vCenter sélectionnée parmi les plates-formes ACI, AWS, Azure et GCP

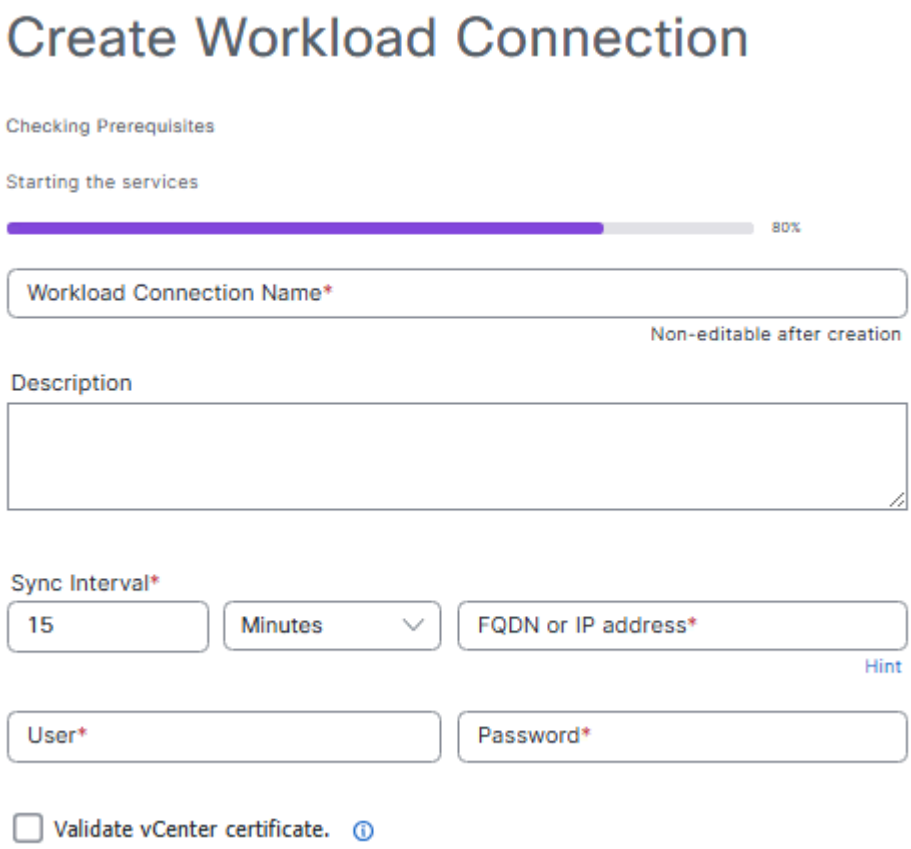
5. Sur la page Create Workload Connection, Cisco ISE vérifie si les services Workload Connector sont en cours d'exécution avant d'accepter les détails de connexion.

Si les services ne sont pas encore en cours d'exécution, la page signale que les services du connecteur de charge globale ne sont pas en cours d'exécution.



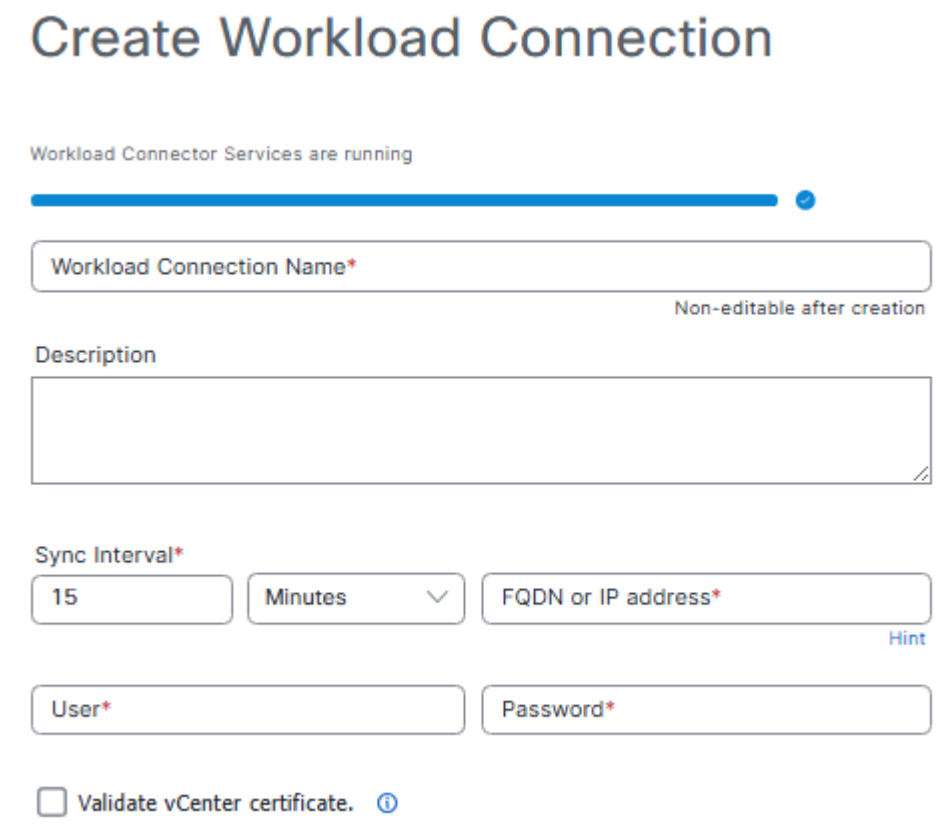
Page Créer une connexion de charge globale signalant que les services du connecteur de charge globale ne sont pas en cours d'exécution

Cisco ISE démarre ensuite les services automatiquement et affiche la progression.



Page Créer une connexion de charge globale affichant le démarrage des services du connecteur de charge globale

Patientez jusqu'à ce que la page indique que les services Workload Connector sont en cours d'exécution. Les champs Détails de la connexion ne peuvent être renseignés qu'après la réussite de cette vérification.

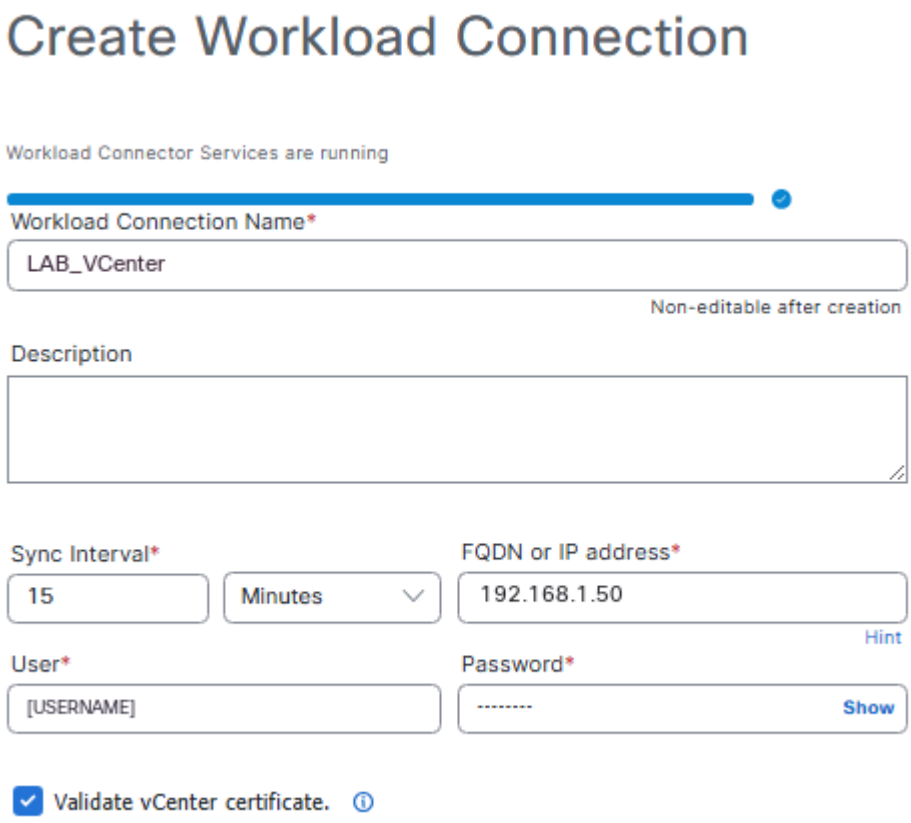


Page Créer une connexion de charge globale confirmant l'exécution des services du connecteur de charge globale

6. Entrez les détails de la connexion :

Champ	Description
Nom de connexion de charge globale	Nom unique qui utilise des lettres, des chiffres et des traits de soulignement. 32 caractères maximum, pas d'espaces. Cet exemple utilise LAB_VCenter.
Description	Description de la connexion.
Intervalle de synchronisation	Fréquence à laquelle Cisco ISE actualise les données de vCenter. La plage valide est comprise entre 60 secondes et 7 jours. La valeur par défaut est 15 minutes. Des intervalles plus courts actualisent les données plus fréquemment, mais peuvent affecter les performances.
FQDN ou adresse IP	Nom d'hôte ou adresse IP de vCenter, par exemple [VCENTER_FQDN] ou [VCENTER_IP_ADDRESS]. Cette valeur doit

Champ	Description
	correspondre à l'autre nom du sujet du certificat du point d'extrémité vCenter.
Utilisateur	Nom d'utilisateur du compte vCenter, [USERNAME].
Mot de passe	Mot de passe du compte vCenter, [MOT DE PASSE].
Valider le certificat vCenter	Facultatif. Valide le certificat et importe le certificat racine vCenter dans le magasin de certificats sécurisés Cisco ISE. Lors de l'importation, vérifiez également l'authentification des services Cisco. La validation des certificats est recommandée pour les environnements de production.



Page Créer une connexion de charge globale avec les champs détaillés de connexion vCenter complétés et la case à cocher Valider le certificat vCenter activée

Dans cette image, le champ Utilisateur affiche un espace réservé. Saisissez les informations d'identification qui s'appliquent à votre environnement.

Remarque : Cisco ISE valide les informations que vous entrez. Si un détail est incorrect, Cisco ISE renvoie l'erreur « Test connection failed ».

7. Cliquez sur Suivant. Cisco ISE teste la connexion et confirme le résultat avec le message Test connection is successful.

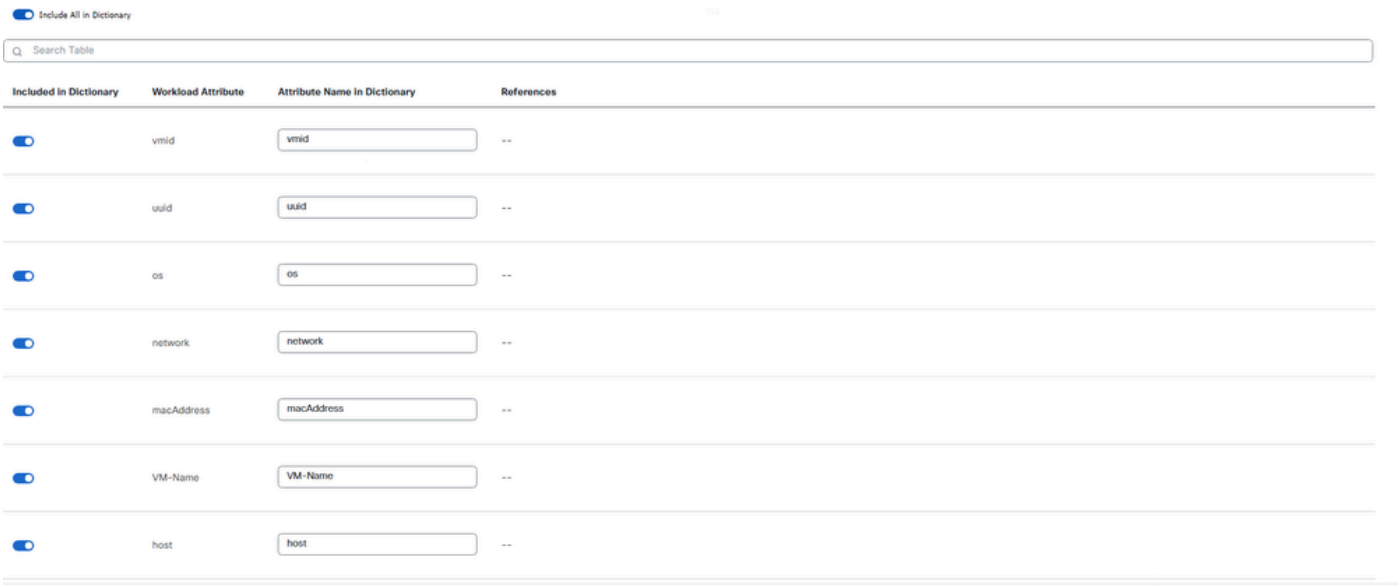


Notification de réussite confirmant que la connexion de test à vCenter a réussi

Notification de réussite confirmant que la connexion de test à vCenter a réussi

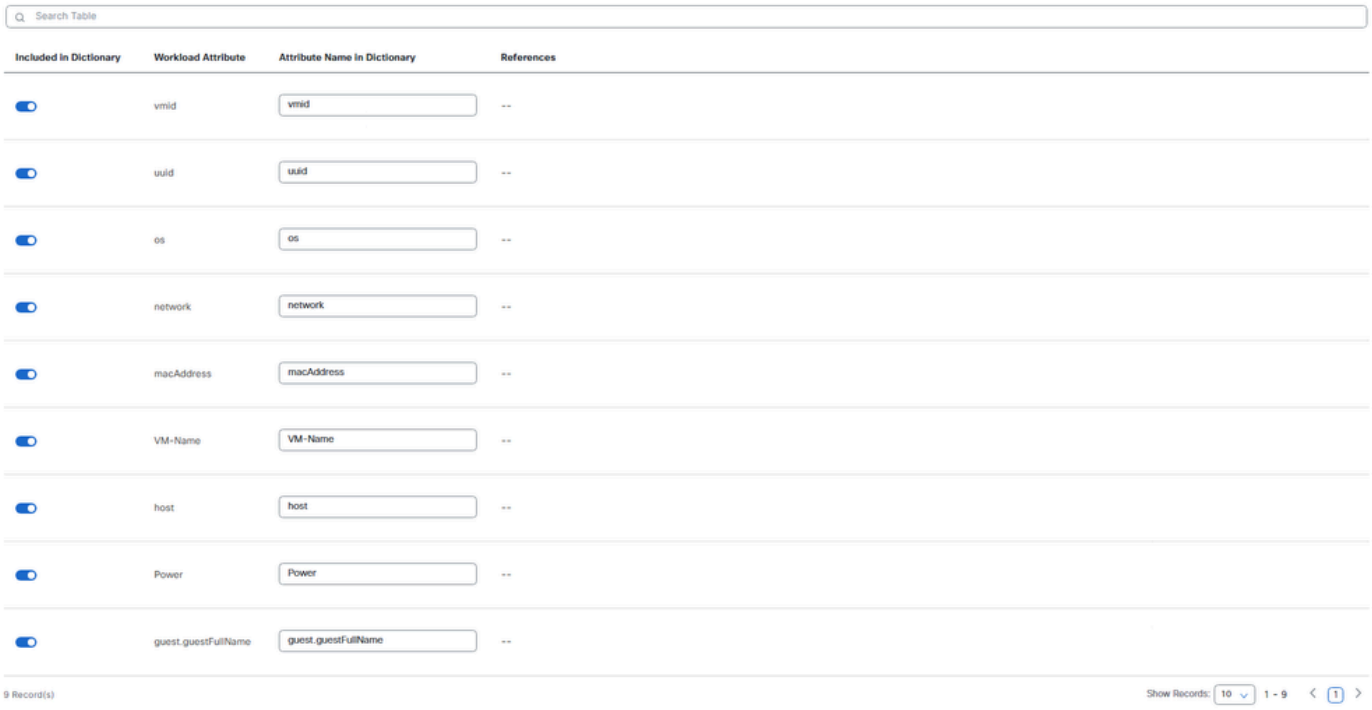
8. Sur la page Manage Attributes, choisissez les attributs vCenter à ajouter au dictionnaire Cisco ISE. Dans cet exemple, assurez-vous que l'attribut os est inclus. Cliquez ensuite sur Next.

- Pour inclure tous les attributs appris à la fois, activez la bascule Tout inclure dans le dictionnaire.
- Pour renommer un attribut, modifiez le champ Nom de l'attribut dans le dictionnaire.
- Vous devez ajouter au moins un attribut avant de pouvoir continuer.
- Noms d'attribut contenant des caractères spéciaux tels que ^, =, ", \, |, :, [, ou] ne sont pas valides et ne peuvent pas être ajoutés.



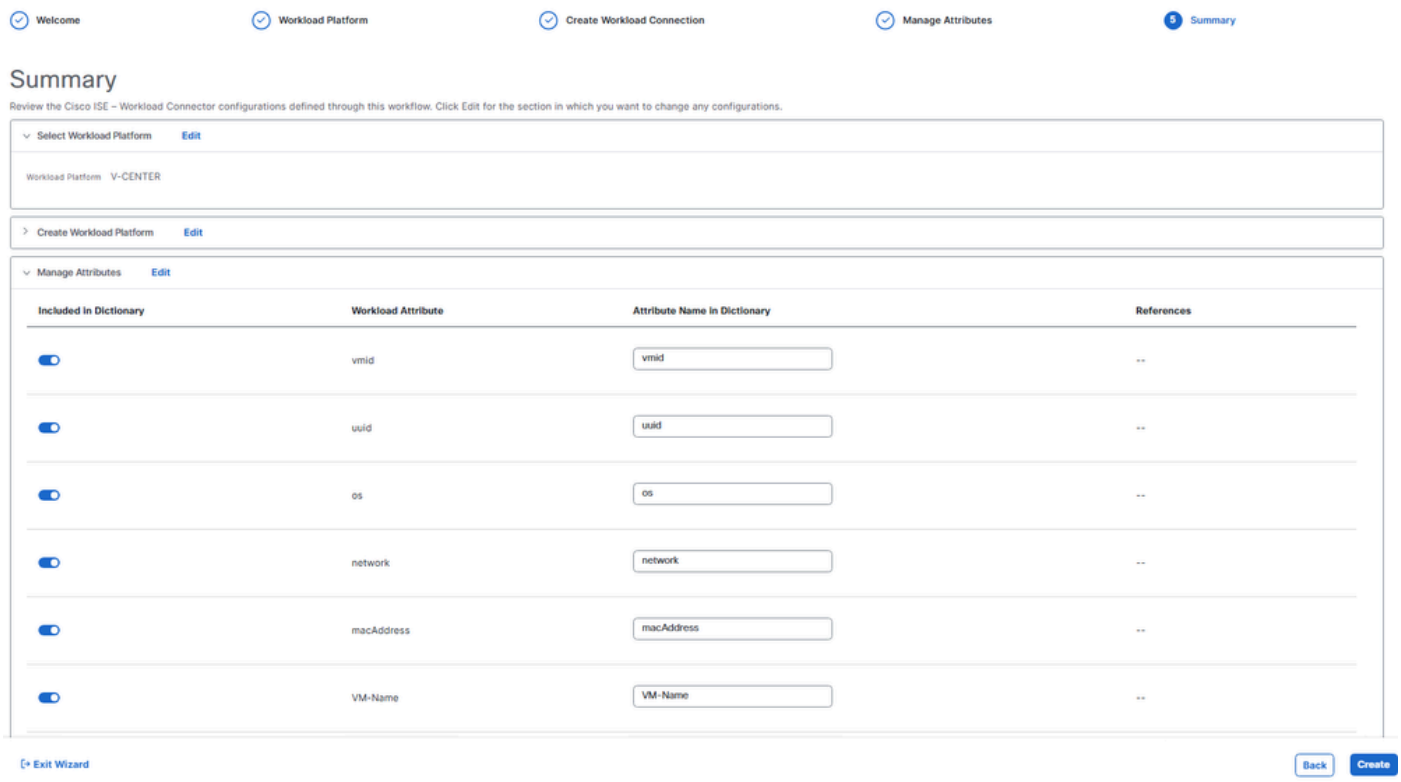
Page Gérer les attributs avec l'option Inclure tout dans le dictionnaire activée et les attributs vCenter acquis répertoriés

Faites défiler la liste pour passer en revue tous les attributs que la connexion a appris de vCenter, tels que vmid, uuid, os, network, macAddress, VM-Name, host, Power et guest.guestFullName.



La page Gérer les attributs a défilé pour afficher la liste complète des attributs vCenter acquis et le nombre d'enregistrements

9. Sur la page Summary, vérifiez la configuration. Cliquez sur Modifier à côté d'une section pour modifier ses valeurs.



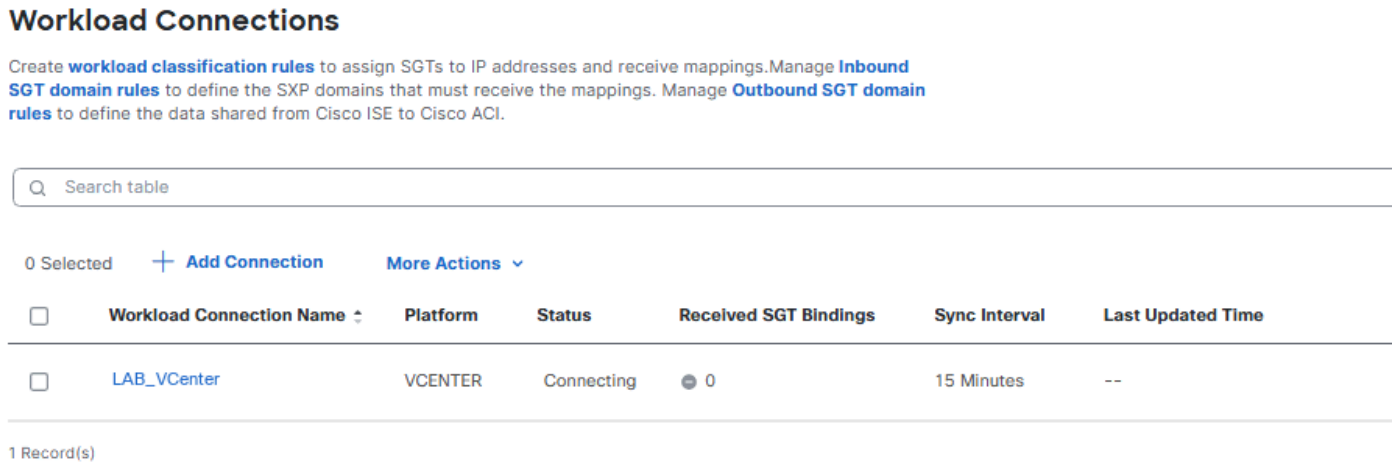
Page Récapitulatif indiquant la plate-forme de charge de travail V-CENTER sélectionnée et les attributs inclus dans le dictionnaire

10. Cliquez sur Créer. Cisco ISE confirme le résultat avec le message Connexion créée avec succès.



Notification de réussite confirmant que la connexion de charge globale a été créée

Le nouveau connecteur vCenter apparaît sur la page Connexions de charge globale. L'état est Connexion pendant que Cisco ISE établit la session avec vCenter.



Page Connexions de charge globale répertoriant le nouveau connecteur vCenter à l'état Connexion

Étape 2. Ajout d'attributs vCenter au dictionnaire (facultatif)

Complétez cette étape uniquement si vous souhaitez ajouter un attribut personnalisé. Les attributs que vous choisissez lors de l'étape Gérer les attributs sont ajoutés automatiquement au dictionnaire vCenter, de sorte que l'intégration fonctionne sans aucune action ici. Les attributs de dictionnaire peuvent également être gérés à tout moment après la création de la connexion :

1. Choisissez Work Centers > TrustSec > Integrations > Workload Connectors.
2. Cliquez sur Dictionnaire d'attributs.
3. Cliquez sur Ajouter un attribut.
4. Activez la bascule Inclure dans le dictionnaire.
5. Dans le champ Attribut de charge globale, saisissez le nom de l'attribut, tel que os.
6. Dans le champ Nom de l'attribut dans le dictionnaire, saisissez le nom à afficher.
7. Cliquez sur Save.

Remarque : Soyez conscient de ce comportement de dictionnaire : Un dictionnaire est créé par type de connexion. Tous les connecteurs vCenter partagent un dictionnaire vCenter unique. Les attributs ne sont pas supprimés automatiquement lorsqu'une connexion est supprimée. Tout attribut qui n'est pas utilisé peut être supprimé manuellement. Les attributs peuvent être importés à partir du fournisseur et les attributs qui ne sont pas présents dans le fournisseur peuvent être ajoutés manuellement.

Étape 3. Classification des charges de travail en SGT

Les règles de classification de charge globale évaluent les attributs de charge globale, y compris les balises vCenter qui ont été importées, et attribuent des balises SGT. Cette étape fournit la valeur de segmentation de l'intégration.

L'affectation des balises de groupe de sécurité se comporte comme décrit dans les éléments suivants :

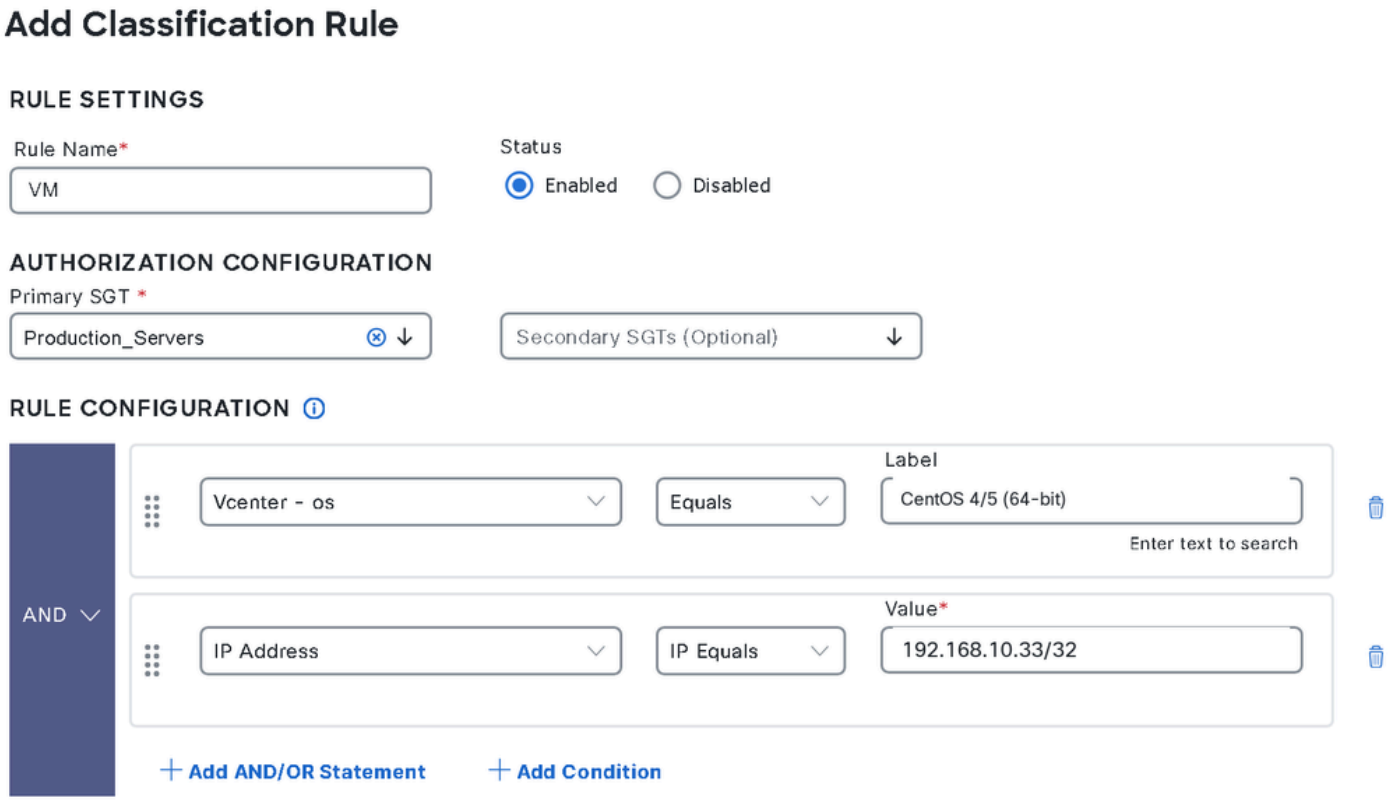
- Le SGT principal est marqué comme groupe de sécurité dans la rubrique de session pxGrid et est utilisé pour publier des mappages IP-à-SGT via SXP.
- Les balises SGT secondaires sont incluses dans la rubrique de session pxGrid sous la forme d'un tableau ordonné nommé Secondary Security Groups.
- Si plusieurs règles correspondent et attribuent plusieurs SGT primaires, seul le premier SGT attribué est traité comme principal. Les balises de groupe de sécurité restantes deviennent secondaires.

Pour créer une règle de classification pour cet exemple :

1. Choisissez Work Centers > TrustSec > Integrations > Workload Classification.
2. Cliquez sur Ajouter une règle de classification.
3. Dans la zone RULE SETTINGS, entrez un nom de règle et définissez Status sur Enabled.
4. Dans la zone AUTHORIZATION CONFIGURATION, dans la liste déroulante Primary SGT, sélectionnez le SGT que la règle attribue, tel que [SGT_NAME]. Cet exemple attribue le SGT Production_Servers.
5. Dans la liste déroulante Secondary SGTs (Optional), sélectionnez éventuellement un ou plusieurs SGT secondaires.
6. Dans la zone RULE CONFIGURATION, créez la condition de correspondance. Dans la liste déroulante des attributs, sélectionnez un attribut vCenter importé, tel que Vcenter - os, choisissez l'opérateur Égal, puis entrez la valeur à faire correspondre. Cet exemple correspond à CentOS 4/5 (64 bits).
7. Pour affiner la règle, cliquez sur Add Condition et combinez les conditions avec AND ou OR. Cet exemple ajoute une condition IP Address qui utilise l'opérateur IP Equals pour restreindre la règle à l'adresse d'hôte unique 192.168.10.33/32.
8. Cliquez éventuellement sur Aperçu pour passer en revue les détails des balises de groupe de sécurité et les charges de travail auxquelles la règle correspond.

9. Cliquez sur Ajouter.

⚠ Mise en garde : L'opérateur Est égal à nécessite la valeur d'attribut complète. vCenter signale le système d'exploitation invité comme une chaîne descriptive complète, telle que CentOS 4/5 (64 bits), et non comme un nom court tel que CentOS. Une règle qui teste Equals CentOS par rapport à cette valeur ne correspond jamais et échoue silencieusement : le connecteur continue d'importer des charges de travail, mais aucun SGT n'est attribué. Vérifiez la valeur exacte dans la Visibilité du contexte avant de créer la règle, comme décrit dans la section Vérifier, ou utilisez un opérateur tel que Contient si vous voulez faire correspondre une famille de systèmes d'exploitation invités.



Page Add Classification Rule attribuant le SGT principal Production_Servers lorsque l'attribut vCenter os est égal à CentOS 4/5 (64 bits) et que l'adresse IP est égale à 192.168.10.33/32

Répétez ces étapes pour chaque groupe supplémentaire de charges de travail que vous souhaitez classer et attribuez une SGT principale différente à chaque règle.

✎ Remarque : Connaître le comportement des règles : Les règles peuvent être réorganisées par glisser-déplacer. L'ordre détermine la priorité. Une nouvelle règle ou une règle en

double peut être insérée avant ou après une règle existante. La règle de classification par défaut se trouve toujours en bas de la liste, est désactivée par défaut et est mappée à la SGT principale inconnue. Utilisez l'option Aperçu pour consulter les détails des balises de groupe de sécurité et les règles de correspondance avant d'enregistrer.

Étape 4. Liaisons de route avec les règles de domaine SGT entrantes et sortantes

Les domaines SGT contrôlent les parties du réseau qui reçoivent des liaisons SGT spécifiques. Si aucune règle entrante n'est définie, les liaisons reçues des connecteurs de charge de travail sont envoyées au domaine SGT par défaut.

Ajouter une règle de domaine SGT entrante :

1. Choisissez Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules.
2. Dans l'onglet Inbound SGT Domain Rules, cliquez sur Add Inbound Rule.
3. Dans la zone Paramètres de règle, entrez un nom de règle.
4. Cliquez sur Enabled.
5. Dans la liste déroulante Destination, sélectionnez les domaines SGT qui doivent recevoir les liaisons. Pour ajouter un domaine, utilisez Create SGT Domain.
6. Dans la zone Rule Configuration, créez la condition à partir d'attributs tels que SGT Name, Source, IP Address, ou tout attribut vCenter qui a été ajouté au dictionnaire, tel que os. Combinez les conditions avec AND et OR si nécessaire.
7. Cliquez sur Add, puis sur Save.

Ajouter une règle de domaine SGT sortante :

1. Sur la même page, ouvrez l'onglet Outbound SGT Domain Rules et cliquez sur Add Outbound Rule.
2. Entrez un nom de règle et cliquez sur Enabled (Activé).
3. Dans la liste déroulante Destination, sélectionnez les destinations vers lesquelles les SGT doivent être envoyées.
4. Dans la zone Rule Configuration, créez la condition à partir de SGT Domains, SGT Name, ou IP Address.
5. Dans la zone Configuration du contrat, vous pouvez éventuellement affecter des contrats Consommés et Fournis aux groupes de sécurité partagés.
6. Cliquez sur Add, puis sur Save.

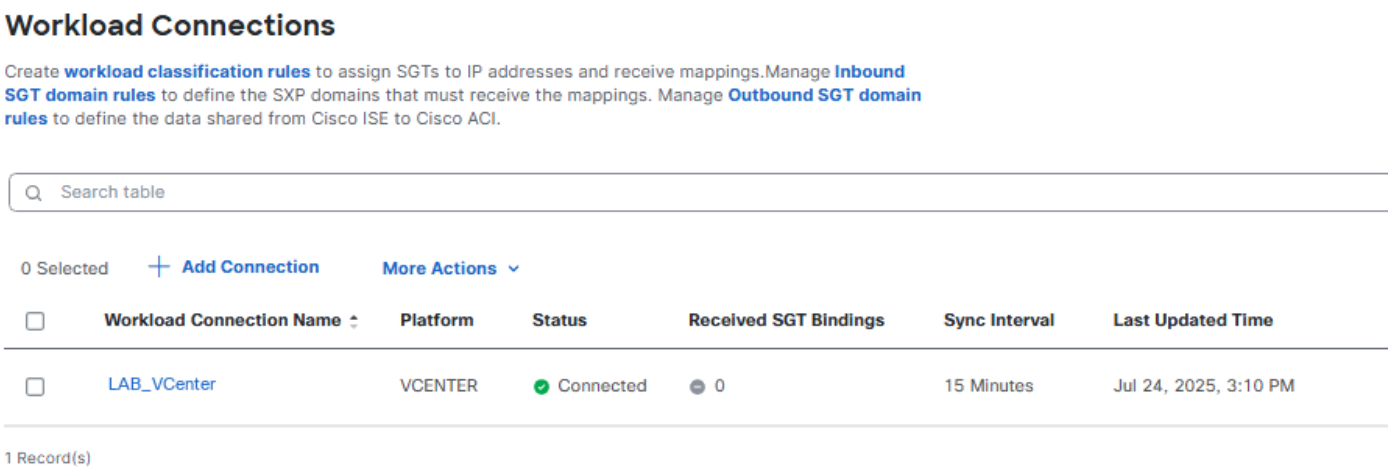
Utilisez l'option Preview pour passer en revue les liaisons IP-SGT correspondantes pendant que vous ajoutez ou modifiez des règles entrantes et sortantes.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de l'état de la connexion

Choisissez Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections et vérifiez que la connexion vCenter est répertoriée avec un état Connected. Cette page vous permet également de vous reconnecter, de suspendre ou de supprimer une connexion.



Page Connexions de charge globale affichant le connecteur vCenter avec l'état Connecté, le nombre de liaisons SGT reçues, l'intervalle de synchronisation et l'heure de la dernière mise à jour

La colonne Received SGT Bindings indique 0 dans cette image car la capture a été effectuée avant qu'une règle de classification corresponde à une charge de travail. Un état Connecté associé à un nombre de liaisons nul signifie que Cisco ISE a atteint vCenter avec succès, mais n'a encore attribué aucun SGT. Une fois qu'une règle correspond, cette colonne indique le nombre de liaisons que Cisco ISE a dérivées.

Vérification des groupes de sécurité

Choisissez Work Centers > TrustSec > Components > Security Groups et vérifiez que les balises de groupe de sécurité attendues existent. Pour cet exemple, vérifiez que le SGT

Production_Servers existe.

Vérification des liaisons IP-SGT

Choisissez Work Centers > TrustSec > SXP > SGT Bindings et vérifiez que les adresses IP de la charge de travail sont liées aux SGT corrects, avec la source correcte et la règle de classification appliquée.

Vérification des sessions en direct de la charge globale

Choisissez Operations > Workloads > Live Session, qui ouvre la page Workload Live Sessions. Les sessions en direct ne peuvent être affichées que sur le noeud principal d'administration des stratégies (PAN). Sur cette page, les sessions peuvent être filtrées par type de connecteur, les colonnes peuvent être affichées, masquées et réorganisées, les résultats peuvent être triés, les filtres peuvent être enregistrés et les données peuvent être exportées au format CSV ou PDF.

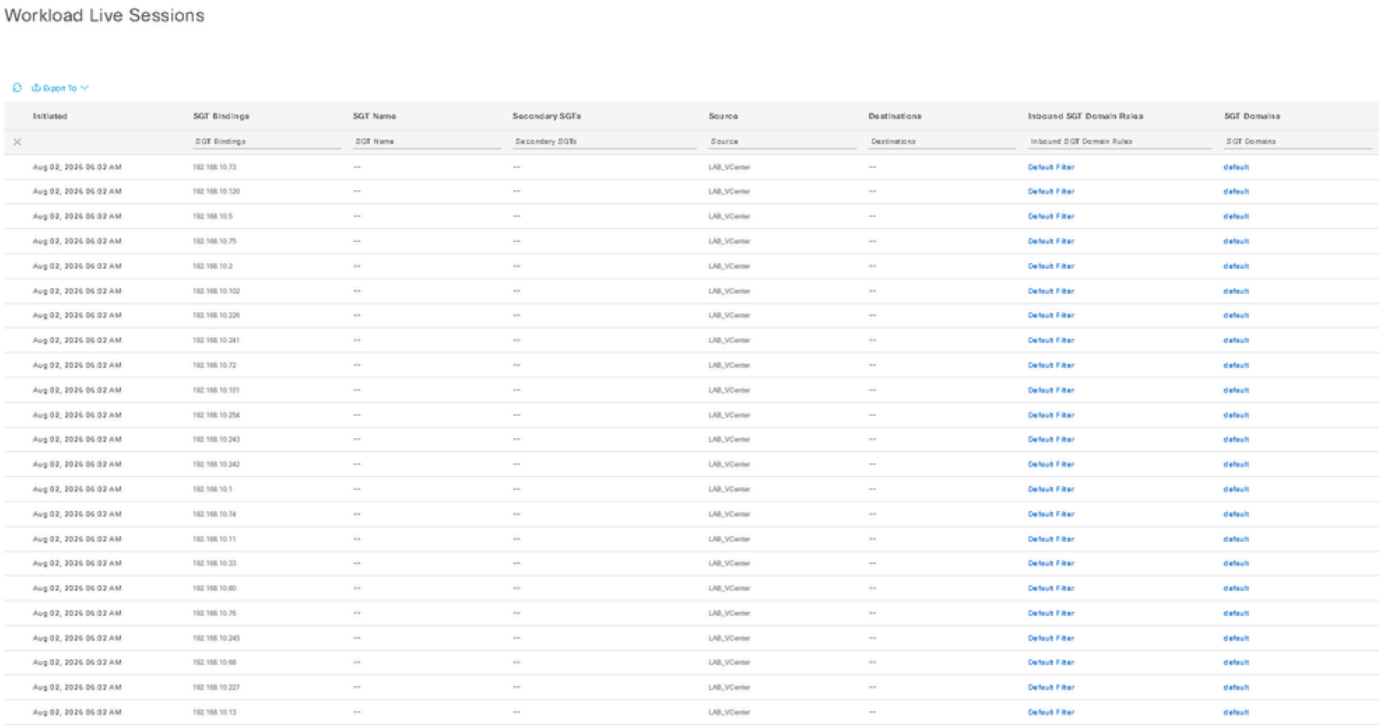


Tableau Sessions en direct de charge globale répertoriant une ligne par charge globale apprise, avec l'horodatage Initiated, l'adresse IP des liaisons SGT, les colonnes vides SGT Name, Secondary SGTs et Destinations, le nom de la connexion source LAB_VCenter et les liens Inbound SGT Domain Rules et SGT Domains indiquant Default Filter et default

Remarque : Cette capture est rognée aux colonnes qui transportent des données dans cet exemple. Les colonnes Règles de domaine SGT sortantes et Règles de classification de charge globale se poursuivent à droite de la zone visible et sont vides sur chaque ligne, tout comme les colonnes spécifiques à l'ACI situées au-delà. Cette page a été capturée dans une session de travaux pratiques ultérieure à celle des pages de configuration du connecteur, de sorte que ses horodatages Initiated ne correspondent pas à l'heure de la dernière mise à jour indiquée précédemment sur la page Connexions de charge globale.

Chaque ligne représente une charge de travail que Cisco ISE a apprise d'un connecteur. Utilisez ces colonnes pour confirmer l'intégration :

Colonne	Ce qu'il confirme
Initié	Heure à laquelle Cisco ISE a appris la session. Des horodatages récents confirment que le connecteur est en cours d’interrogation.
Liaisons SGT	Adresse IP de la charge de travail que Cisco ISE a reçue de vCenter.
Source	Connexion de charge globale ayant signalé la session. Confirme de quel connecteur proviennent les données.
Règles de domaine SGT entrant et domaines SGT	Règle de domaine et domaine SGT appliqués à la session. Sélectionnez un lien pour afficher la règle correspondante.
Nom SGT, SGT secondaires et règles de classification de charge de travail	Les balises SGT attribuées à la charge de travail et la règle qui les a attribuées. Ces colonnes restent vides pour les charges de travail pour lesquelles aucune règle de classification ne correspond.

Utilisez les contrôles Refresh, Show et Within dans le coin supérieur droit de la page, à droite de la zone rognée, pour définir l'intervalle de rafraîchissement, le nombre d'enregistrements et la fenêtre de temps.

Dans cette image, la colonne SGT Bindings est entièrement remplie tandis que les champs SGT Name et Secondary SGT sont vides sur chaque ligne, car la capture a été effectuée avant qu'une règle de classification ne corresponde. La colonne Règles de classification de charge globale, située en dehors de la zone rognée, est vide pour la même raison. Cette combinaison est un diagnostic utile en soi : il confirme que le connecteur récupère correctement les charges de travail de vCenter et que le problème réside dans les conditions de la règle plutôt que dans la connexion. Lorsque vous le voyez, revenez à l'étape 3 et comparez les valeurs de correspondance aux

valeurs d'attribut que Context Visibility rapporte, comme décrit dans la section Attention de cette étape.

Vérification de la visibilité des charges de travail dans Context Visibility

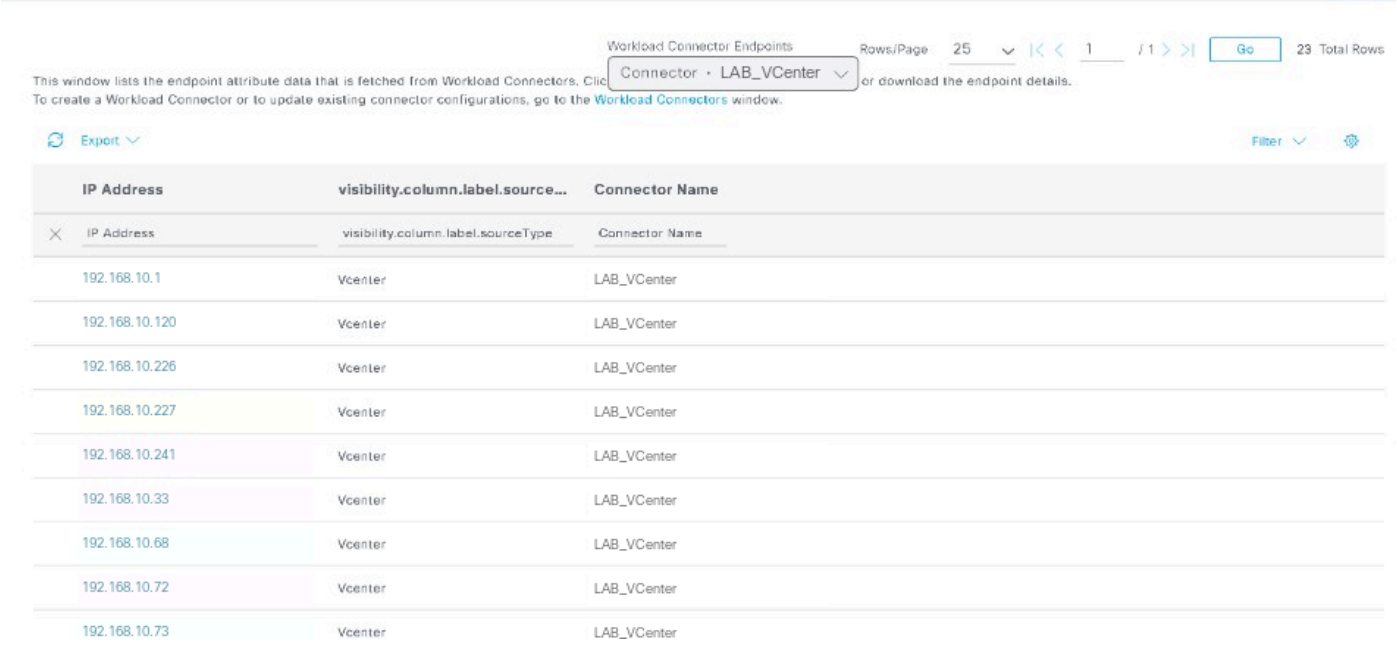
⚠ Version requise : Le tableau de bord Workload Connector Endpoints est disponible à partir de Cisco ISE 3.5 Patch 3. Sur Cisco ISE 3.4, utilisez la page Workload Live Sessions décrite dans la section précédente.

Cisco ISE fournit un tableau de bord dédié aux terminaux du connecteur de charge de travail dans Context Visibility. Il collecte, analyse et consigne les données d'attribut de point de terminaison collectées à partir des connecteurs de charge de travail dans une vue unique et filtrable.

Pour ouvrir la vue :

1. Dans l'interface utilisateur graphique de Cisco ISE, choisissez Context Visibility > Endpoints.
2. Ouvrez l'onglet Terminaux du connecteur de charge globale. Si l'onglet n'est pas visible dans la bande d'onglets, cliquez sur More.
3. Dans la liste déroulante Connecteur, sélectionnez la connexion de charge globale dont vous souhaitez vérifier les points de terminaison.

La fenêtre répertorie les données d'attribut de point de terminaison extraites des connecteurs de charge globale. Chaque ligne identifie un point de terminaison par adresse IP, type de source et nom de connecteur.



Vue Points de terminaison du connecteur de charge globale sous Visibilité du contexte, répertoriant les points de terminaison de

charge globale vCenter par adresse IP, type de source et nom de connecteur, avec la liste déroulante Connecteur définie sur LAB_VCenter, l'option Exporter, les contrôles Lignes/Page et Pagination, et un nombre total de 23 lignes

Dans cette vue, vous pouvez :

- Filtrer la liste. Utilisez la ligne de filtre sous les en-têtes de colonne pour affiner les résultats par adresse IP, type de source ou nom de connecteur. Les filtres s'additionnent, de sorte que chaque valeur que vous appliquez affine davantage le jeu de résultats.
- Parcourez les résultats. Utilisez le contrôle Rows/Page et les flèches de pagination pour modifier la taille de la page et vous déplacer entre les pages. Le nombre total de points d'extrémité apparaît à droite des flèches, affiché ici comme 23 lignes totales.
- Exportez les données. Cliquez sur Export pour télécharger les données de point de terminaison répertoriées.
- Inspecter un terminal. Cliquez sur l'adresse IP d'un point d'extrémité pour ouvrir le volet Détails.

Le volet Détails répertorie tous les attributs que Cisco ISE contient pour le point de terminaison sélectionné. Cliquez sur Download pour enregistrer les détails de l'attribut ou cliquez sur Cancel pour fermer le volet.

Details

LAB_VCenter_192.168.10.1

ATTRIBUTES

Power: running

VM-Name: [VM_NAME]

host: [HOST_ID]

macAddress: 00:50:56:XX:XX:XX

network: [NETWORK_NAME]

os: CentOS 4/5 (64-bit)

uuid: [VM_UUID]

vmid: [VM_ID]

vmtype: vmware

correlationId: 192.168.10.1

source: LAB_VCenter

ipAddress: 192.168.10.1

connectorType: ExternalConnector

SourceType: Vcenter

Cancel

Download

Volet déroulant Détails pour un point de terminaison de charge de travail sélectionné, intitulé Détails au-dessus du nom du connecteur et de l'adresse du point de terminaison, avec la liste ATTRIBUTS des propriétés vCenter collectées par Cisco ISE pour cette machine virtuelle et les contrôles Annuler et Télécharger

Le volet est identifié par le nom de connexion de la charge globale et l'adresse du point de terminaison, représentés ici par LAB_VCenter_192.168.10.1. Pour un point de terminaison de charge globale vCenter, les attributs incluent les propriétés de machine virtuelle apprises de vCenter, telles que Power, VM-Name, host, macAddress, network, os, uuid, vmid et vmtype, ainsi que les métadonnées de connecteur corrélationId, source, ipAddress, connectorType et SourceType. Toutes les balises vCenter personnalisées que vous avez ajoutées au dictionnaire s'affichent également ici.

Ce volet est la source faisant autorité pour les valeurs auxquelles vos règles de classification doivent correspondre. Sa vérification en premier lieu permet d'éviter l'échec le plus courant dans ce flux de travail. Dans cette image, os lit CentOS 4/5 (64 bits), qui est la chaîne complète qu'une condition Equals doit reproduire. Lisez la valeur ici avant d'écrire la règle à l'étape 3, plutôt que d'adopter une forme abrégée telle que CentOS.

Remarque : Un maximum de 50 attributs est affiché pour chaque point d'extrémité.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Problèmes courants

Symptôme	Cause probable	Action
"Echec du test de connexion" pendant la configuration du connecteur.	Un ou plusieurs détails de connexion sont incorrects ou un prérequis n'est pas satisfait.	Vérifiez le nom de domaine complet (FQDN) ou l'adresse IP et assurez-vous qu'elle correspond au certificat SAN. Vérifiez le nom d'utilisateur et le mot de passe, vérifiez le paramètre de validation du certificat

Symptôme	Cause probable	Action
		et vérifiez que les conditions préalables de contournement du proxy et de synchronisation de l'heure sont remplies.
Le connecteur est créé mais aucune donnée n'est importée.	Cisco ISE ne peut pas atteindre public.ecr.aws.	Vérifiez que le proxy ou le pare-feu autorise le trafic HTTPS sur le port TCP 443 vers cette URL.
Les charges de travail sont importées mais aucune SGT n'est attribuée et les liaisons de SGT reçues restent à 0.	Une condition de règle de classification ne correspond pas à la valeur d'attribut réelle. Une condition Égal à testée par rapport à une valeur partielle, telle que CentOS au lieu de CentOS 4/5 (64 bits), est la cause la plus courante.	Ouvrez le volet Détails dans Visibilité contextuelle, lisez la valeur exacte de l'attribut et corrigez la condition de la règle ou modifiez l'opérateur en Contient. Cette défaillance est silencieuse : aucune alarme n'est déclenchée, car le connecteur lui-même est sain.
La connexion passe à l'état Suspendu.	Tous les SGT associés à la connexion ont été supprimés.	Recréez les balises SGT requises et rétablissez la connexion. Les liaisons SXP et les données de session MnT associées sont supprimées lorsque la connexion est interrompue.
Les détails de connexion sont manquants après un redémarrage PSN.	Les données de session n'ont pas été rechargées.	Interrompez la connexion, puis reconnectez-la.

Activer les journaux de débogage

Définissez la gravité du journal de débogage pour le composant Workload Connector sur DEBUG sur les noeuds PAN, SXP et pxGrid à partir de Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration.

Ces fichiers journaux sont disponibles dans /opt/CSCOcpm/logs :

Fichier journal	Contenu
charges de travail.log	Opérations du connecteur de charge globale
load-conn/*.log	Journaux par connexion
api-service.log	activité de service API
ise-psc.log	Activité du service de stratégie Cisco ISE
pxgriddirect-service.log	activité de service pxGrid Direct
sxp_appserver/sxp.log	distribution de liaison SXP

Alarmes

Cisco ISE génère les alarmes suivantes pour vCenter et d'autres connecteurs cloud :

Alarme	Déclenché lorsque
Échec de la création/connexion de charge globale	La création du connecteur échoue après un événement tel qu'une restauration, une promotion, un événement de haute disponibilité ou une mise à niveau.
Échec de la suppression de connexion de charge globale	La suppression du connecteur échoue.
Erreur du service de connexion de charge globale	Une autre panne de service associée se produit.

Informations connexes

- Connecteurs Cisco ISE Common Policy et Workload
- URL Internet requises par Cisco ISE
- Guide de l'administrateur de Cisco ISE 3.5
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.