Konfigurieren der ISE Workload Connector-Integration mit VMware vCenter

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der Cisco ISE Workload Connector für VMware vCenter konfiguriert wird, um Workload-Kontext zu importieren und eine gruppenbasierte

Segmentierung durchzusetzen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Verwaltung der Cisco ISE
- VMware vCenter-Administration
- Cisco TrustSec-Konzepte, einschließlich Security Group Tags (SGTs), SGT Exchange Protocol (SXP) und pxGrid

Bevor Sie eine vCenter-Workload-Verbindung hinzufügen, stellen Sie sicher, dass diese Bedingungen erfüllt sind.

Cisco ISE

- pxGrid ist auf mindestens einem Knoten in der Bereitstellung aktiviert.
- SXP ist auf mindestens einem Knoten in der Bereitstellung aktiviert.

VMware vCenter

- Ein vCenter-Konto mit schreibgeschützter Berechtigung ist verfügbar. Der Connector führt nur Lesevorgänge aus.
- Die zu importierenden vCenter-Attribute oder -Tags wurden identifiziert. In diesem Dokument wird das os-Attribut als Beispiel verwendet.

Konnektivität

- Für die Cisco ISE steht eine stabile Internetverbindung zur Verfügung, da die Cisco ISE public.ecr.aws erreichen kann. Dies ist für die Workload Connector-Funktion erforderlich. Wenn sich ein Proxyserver oder eine Firewall im Pfad befindet, lassen Sie den HTTPS-Datenverkehr (TCP-Port 443) zwischen der Cisco ISE und dieser URL zu. Wenn diese URL nicht erreichbar ist, funktioniert der Workload Connector nicht wie vorgesehen.
- Wenn ein Proxy für den Internetzugriff verwendet wird und vCenter vor Ort bereitgestellt wird,

konfigurieren Sie eine Proxy-Umgehung für die vCenter-IP-Adresse.

Zertifikate

- Wenn die Zertifikatsvalidierung verwendet wird, muss der für vCenter eingegebene FQDN oder die IP-Adresse mit dem Subject Alternative Name (SAN) des vCenter-Endpunktzertifikats übereinstimmen.
- Das vCenter-Stammzertifikat muss für den Import in den Speicher für vertrauenswürdige Zertifikate der Cisco ISE verfügbar sein.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine (ISE) Version 3.4 für die Konfiguration und Verifizierung von Connectors
- Cisco Identity Services Engine (ISE), Version 3.5 Patch 3, nur für das Context Visibility-Verfahren
- VMware vCenter Server 8.0 Update 3

Anmerkung: Für das Workload Connector Endpoints-Dashboard in Context Visibility ist Cisco ISE 3.5 Patch 3 oder höher erforderlich, sodass die beiden Images in diesem Abschnitt in dieser Version erfasst wurden. Alle weiteren Schritte und Abbildungen in diesem Dokument stammen von der Cisco ISE 3.4.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Moderne Rechenzentren sind dynamisch. Virtuelle Systeme (VMs) werden kontinuierlich erstellt, verschoben und entfernt, und ihre IP-Adressen ändern sich mit ihnen. Sicherheitsrichtlinien, die auf statischen IP-Adressen oder Subnetzen basieren, können mit dieser Änderungsrate nicht Schritt halten, was Lücken bei der Durchsetzung und Transparenz hinterlässt.

Die Cisco ISE löst dieses Problem mithilfe des Common Policy Frameworks und seiner Workload Connectors. Ein Workload Connector stellt eine sichere Verbindung zu einem Rechenzentrum oder einer Cloud-Plattform her, importiert den Kontext der dort ausgeführten Anwendungs-Workloads, normalisiert diesen Kontext in SGTs und teilt das Ergebnis mit dem Rest des Netzwerks, sodass Richtlinien darauf geschrieben werden können.

vCenter beschreibt jedes virtuelle System bereits anhand verschiedener Attribute wie Gastbetriebssystem, Portgruppe und Stromversorgungsstatus. VMware-Administratoren erweitern diese Beschreibung durch benutzerdefinierte Tags, die Metadaten wie Umgebung, Anwendungsebene, Eigentümer oder Geschäftseinheit enthalten. Der vCenter Workload Connector importiert beide und konvertiert sie in SGTs. Dies führt zu drei Ergebnissen:

- Die Richtlinie ist Workload-basiert. Wenn ein virtuelles System verschoben oder neu adressiert wird, bleibt das attributierte SGT erhalten, sodass die Segmentierung ohne manuelle Updates fortgesetzt werden kann.
- Vorhandener Kontext wird wiederverwendet. Die Cisco ISE nutzt die Attribute und Tags, die vCenter bereits pflegt, sodass kein neues Klassifizierungsschema erforderlich ist.
- Konsistente Segmentierung SGTs werden über das TrustSec-fähige Netzwerk verteilt, sodass für jeden Durchsetzungspunkt die gleiche Richtlinie gilt.

In diesem Dokument wird durchgehend ein einziges Beispiel verwendet. Das os-Attribut, das vCenter für jedes virtuelle System meldet und in dieser Übung CentOS 4/5 (64 Bit) liest, wird in die Cisco ISE importiert und mit einer IP-Adressbedingung kombiniert, sodass die entsprechenden Workloads automatisch in einer Sicherheitsgruppe Production_Servers platziert werden. Diese Workloads werden dann nach Gruppenmitgliedschaften und nicht nach manuell verfolgten IP-Adressen segmentiert. Das gleiche Verfahren gilt für alle anderen Attribute oder benutzerdefinierten Tags, die vCenter verfügbar macht.

Schlüsselbegriffe

Anmerkung: VMware ESXi unterstützt keine Tags. Aus diesem Grund kann nur vCenter als Workload-Connector konfiguriert werden. Eigenständige ESXi-Hosts können dies nicht.

Begriff	Definition
TrustSec	Cisco Technologie für gruppenbasierte Segmentierung, bei der Richtlinien nicht für IP-Adressen, sondern für Gruppen geschrieben werden.

Begriff	Definition
SGT (Security Group Tag)	Ein Tag, der eine Gruppe darstellt, z. B. Produktions-Workloads, und als Grundlage für die Richtliniendurchsetzung dient.
SXP (SGT Exchange Protocol)	Das Protokoll, das zur Verteilung von IP-to-SGT-Bindungen an Durchsetzungsgeräte verwendet wird.
pxGrid	Die Cisco Plattform diente früher zur gemeinsamen Nutzung von Kontext, z. B. Sitzungen und SGTs, zwischen der Cisco ISE und anderen Systemen.
Gemeinsame Richtlinie	Das Cisco ISE-Framework, das Verbindungen zu Rechenzentren und Clouds herstellt, deren Kontext in SGTs normalisiert und über verschiedene Domänen hinweg verwendet.
Workload-Connector	Die Cisco ISE-Komponente, die eine Verbindung mit vCenter, AWS, Azure, GCP oder ACI herstellt und Workload-Kontext importiert.

Platzhalter verwendet

Werte in eckigen Klammern sind Platzhalter. Ersetzen Sie sie durch die Werte, die für Ihre Umgebung gelten.

Platzhalter	Beschreibung
[VCENTER_FQDN]	Vollqualifizierter Domänenname des vCenter-Servers.
[VCENTER_IP_ADDRESS]	IP-Adresse des vCenter-Servers
[Benutzername]	Benutzername des schreibgeschützten vCenter-Kontos.
[KENNWORT]	Kennwort des schreibgeschützten vCenter-Kontos.
[SGT_NAME]	Name des Sicherheitsgruppen-Tags, dem eine Klassifizierungsregel zugewiesen wurde.
[VM_NAME]	Name eines virtuellen Systems in vCenter.

Platzhalter	Beschreibung
[VM_UID]	UUID eines virtuellen Systems in vCenter.
[VM_ID]	vCenter-verwalteter Objektverweis eines virtuellen Systems.
[HOST_ID]	vCenter-verwalteter Objektverweis auf einen ESXi-Host.
[NETZWERKNAME]	Name der vCenter-Portgruppe oder des Netzwerks

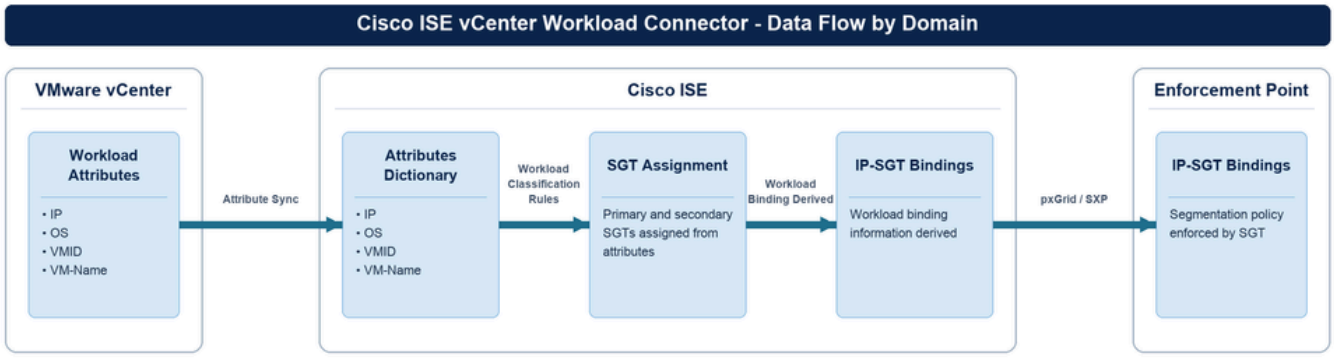
Die Bilder in diesem Dokument stammen aus einer Übung, die den Namen der Workload-Verbindung LAB_VCenter, die vCenter-Adresse 192.168.1.50 und das Workload-Subnetz 192.168.10.0/24 verwendet. Ersetzen Sie dabei die für Ihre Umgebung geltenden Namen und Adressen.

Konfigurieren

Netzwerkdiagramm

Die Integration wandelt vCenter-Metadaten in fünf Stufen in durchsetzbare Richtlinien um:

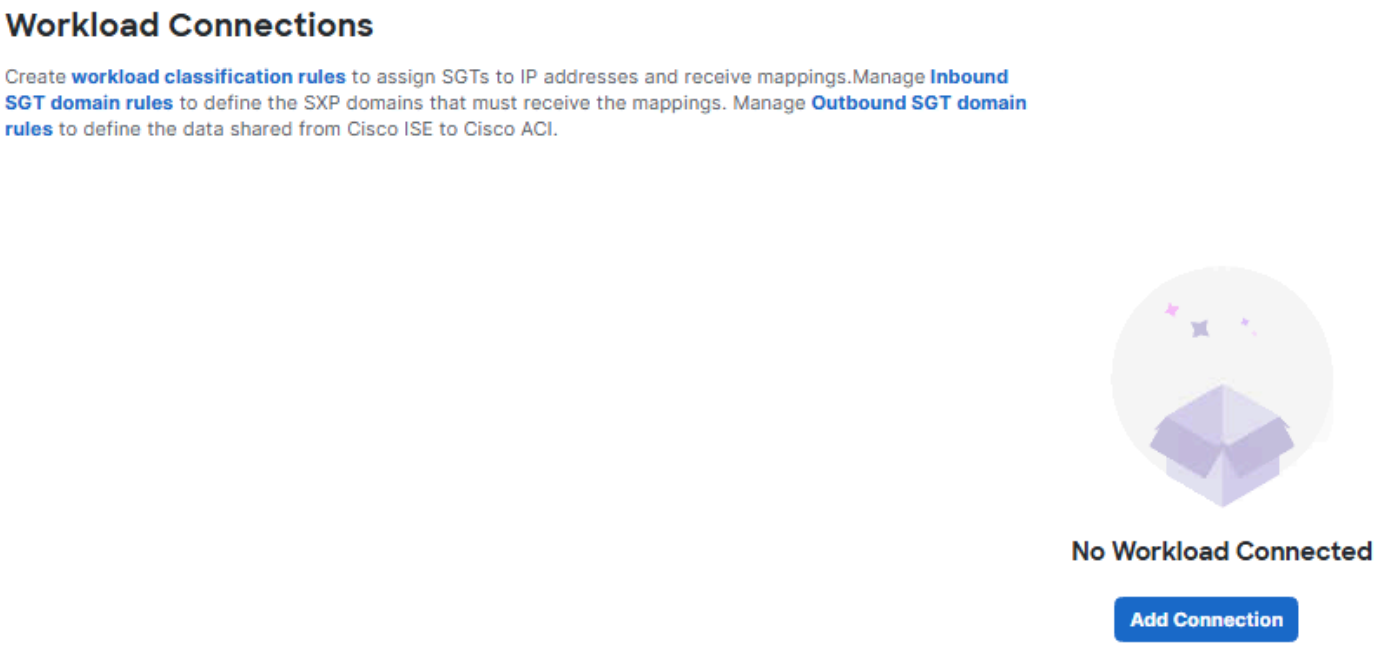
1. Der Cisco ISE vCenter Workload Connector liest die Workload-Attribute und -Tags von vCenter.
2. Die ausgewählten Attribute werden dem Cisco ISE Attributes Dictionary hinzugefügt, damit in Regeln auf sie verwiesen werden kann.
3. Workload-Klassifizierungsregeln bewerten diese Attribute und weisen jedem Workload ein primäres SGT und optional ein oder mehrere sekundäre SGTs zu.
4. Die Cisco ISE leitet IP-to-SGT-Bindungen ab und veröffentlicht sie über SXP und pxGrid. Regeln für eingehende und ausgehende SGT-Domänen steuern, welche SGT-Domänen die Bindungen empfangen und wo sie freigegeben werden.
5. Durchsetzungspunkte wenden die SGTs an, um Datenverkehr zu erlauben oder zu verweigern.



Die Cisco ISE vCenter Workload Connector-Daten fließen über drei Domänen. vCenter bietet Workload-Attribute (IP, OS, VMID, VM-Name); Die Cisco ISE speichert sie im Attributes Dictionary, wendet Workload-Klassifizierungsregeln an, um primäre und sekundäre SGTs zuzuweisen, und leitet IP-SGT-Bindungen ab. Die Bindungen werden über pxGrid und SXP für den Durchsetzungspunkt freigegeben.
Konfigurationen

Schritt 1: Hinzufügen der vCenter-Workload-Verbindung

1. Klicken Sie in der Cisco ISE-GUI auf das Menü-Symbol, und wählen Sie Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections aus.
2. Klicken Sie auf Verbindung hinzufügen.

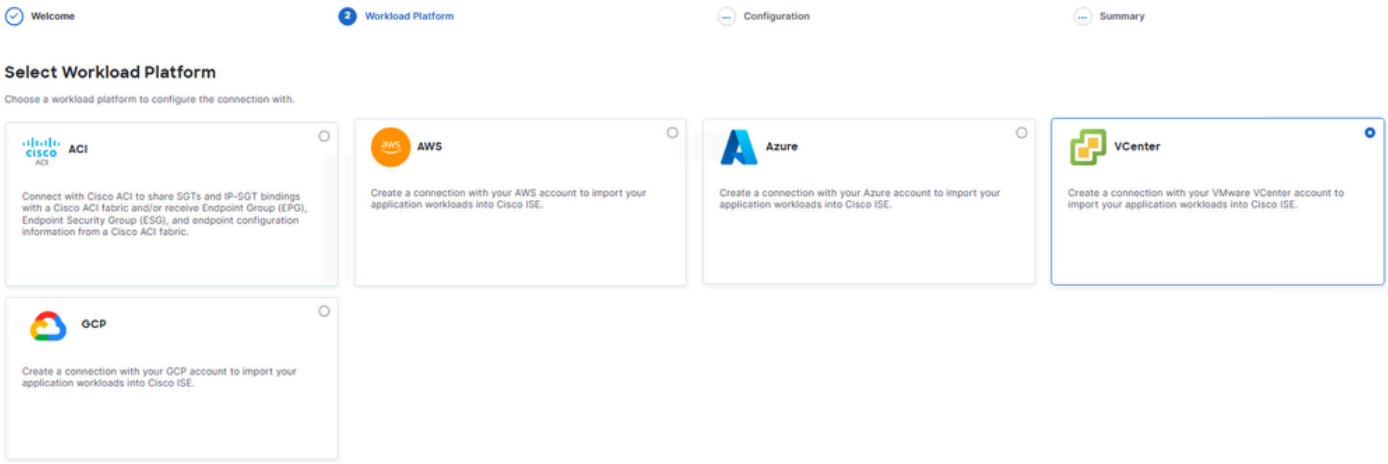


Seite "Workload-Verbindungen" ohne konfigurierte Verbindungen, auf der die Schaltfläche Verbindung hinzufügen angezeigt wird

3. Klicken Sie auf Los geht's.

Workload-Verbindungsassistent Willkommensseite mit den Phasen Willkommen, Workload-Plattform, Konfiguration und Zusammenfassung des Assistenten

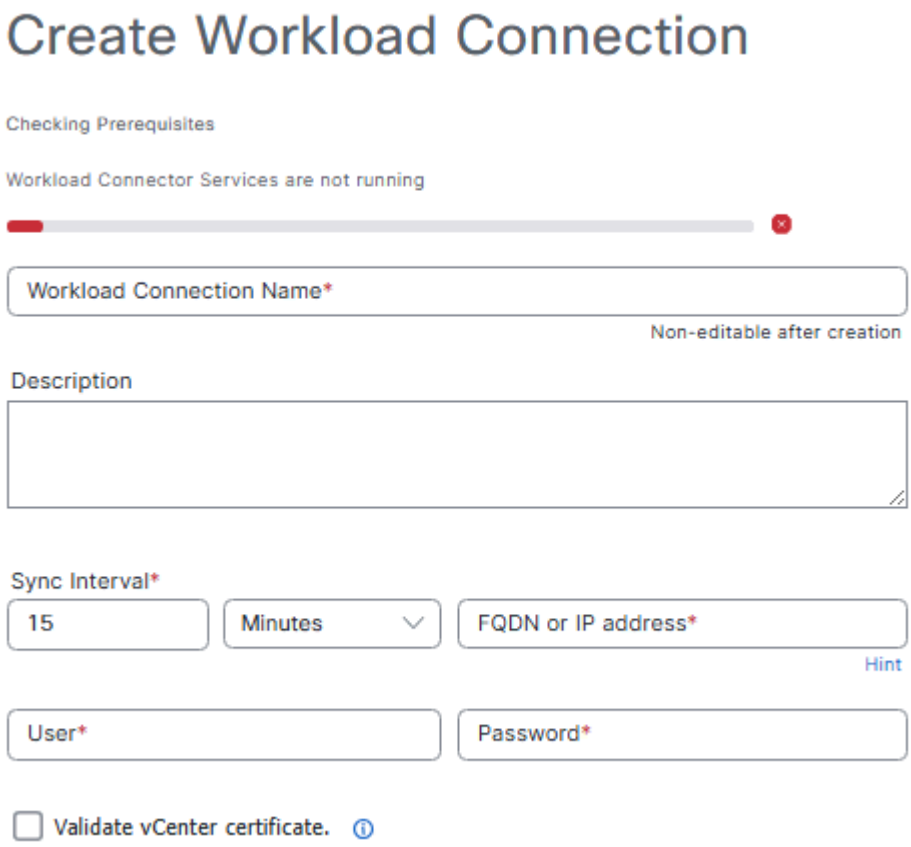
4. Wählen Sie auf der Seite Workload-Plattform auswählen die Option vCenter aus, und klicken Sie dann auf Weiter.



Wählen Sie die Seite "Workload-Plattform" aus, und wählen Sie die vCenter-Option für die ACI-, AWS-, Azure- und GCP-Plattformen aus.

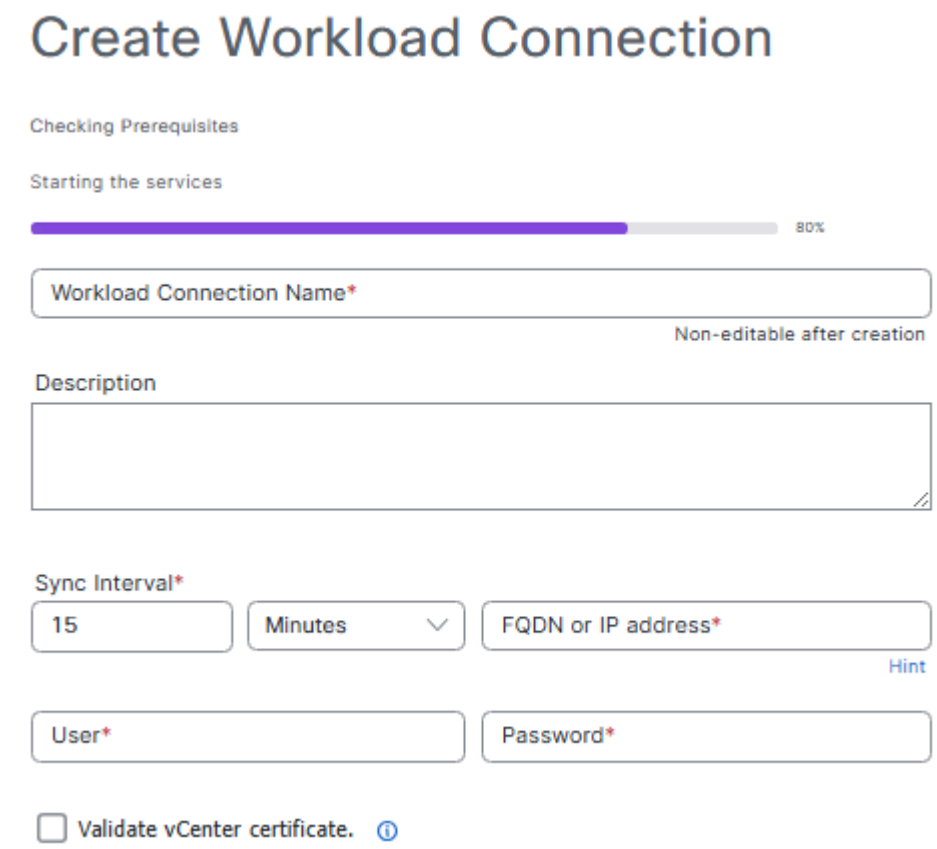
5. Auf der Seite Create Workload Connection (Workload-Verbindung erstellen) prüft die Cisco ISE, ob die Workload Connector-Services ausgeführt werden, bevor sie Verbindungsdetails akzeptiert.

Wenn die Dienste noch nicht ausgeführt werden, wird auf der Seite angezeigt, dass Workload Connector-Dienste nicht ausgeführt werden.



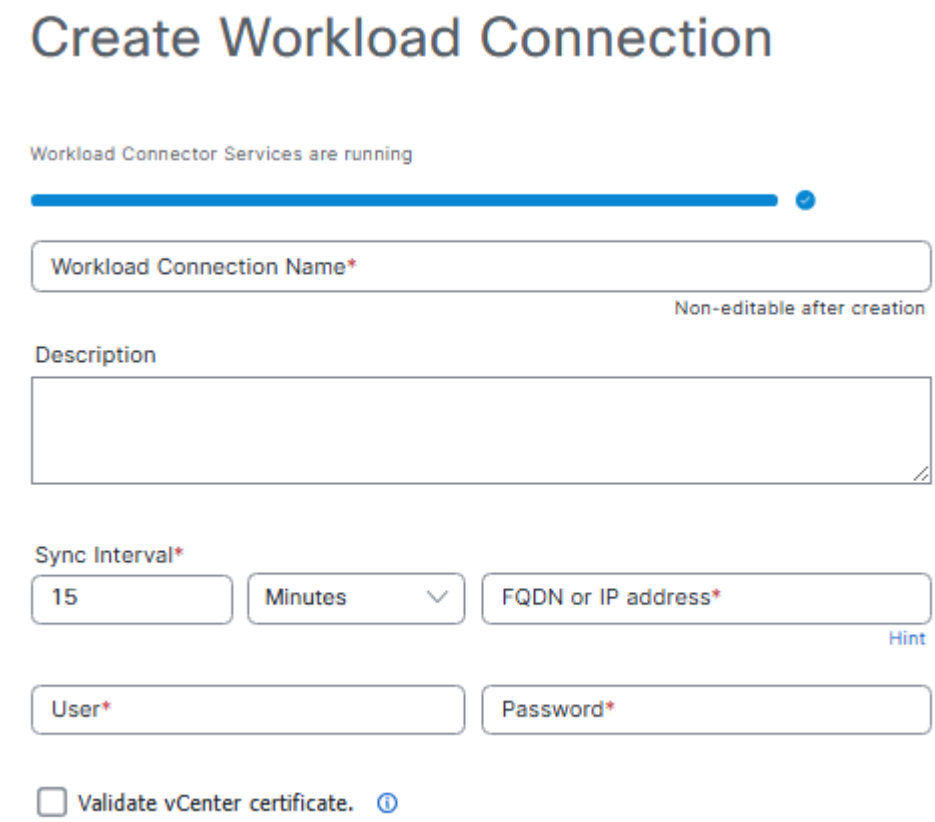
Seite "Workload-Verbindung erstellen", die meldet, dass die Workload Connector-Dienste nicht ausgeführt werden

Die Cisco ISE startet die Services dann automatisch und zeigt den Fortschritt an.



Seite "Workload-Verbindung erstellen" mit den beginnenden Workload Connector-Services

Warten Sie, bis auf der Seite Berichte über die Ausführung von Workload Connector Services angezeigt werden. Die Felder für die Verbindungsdetails können erst nach erfolgreicher Überprüfung ausgefüllt werden.

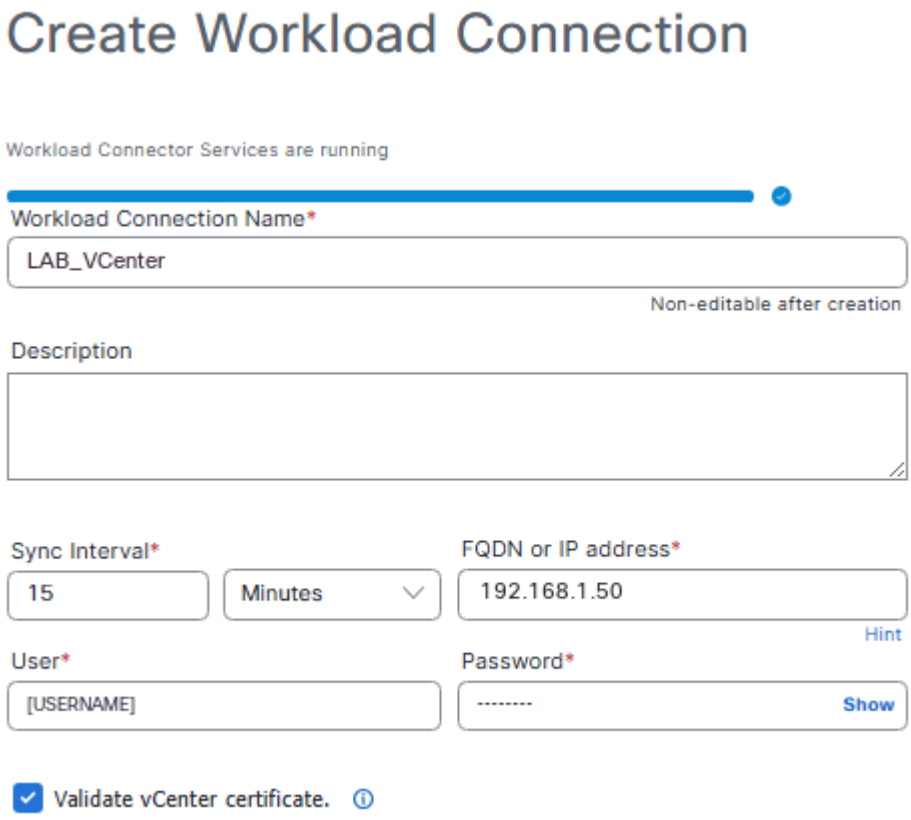


Seite "Workload-Verbindung erstellen", die bestätigt, dass die Workload Connector-Dienste ausgeführt werden

6. Geben Sie die Verbindungsdetails ein:

Feld	Beschreibung
Name der Workload-Verbindung	Ein eindeutiger Name, der Buchstaben, Zahlen und Unterstriche verwendet. Maximal 32 Zeichen, keine Leerzeichen. In diesem Beispiel wird LAB_VCenter verwendet.
Beschreibung	Eine Beschreibung der Verbindung
Synchronisierungsintervall	Legt fest, wie oft die Cisco ISE Daten aus vCenter aktualisiert. Der gültige Bereich liegt zwischen 60 Sekunden und 7 Tagen. Der Standardwert ist 15 Minuten. Kürzere Intervalle aktualisieren Daten häufiger, können jedoch die Leistung beeinträchtigen.
FQDN oder IP-Adresse	Der Hostname oder die IP-Adresse von vCenter, wie

Feld	Beschreibung
	[VCENTER_FQDN] oder [VCENTER_IP_ADDRESS]. Dieser Wert muss mit dem alternativen Antragstellernamen des vCenter-Endpunktzertifikats übereinstimmen.
Benutzer	Den vCenter-Benutzernamen [USERNAME].
Kennwort	Das Kennwort des vCenter-Kontos [PASSWORD].
vCenter-Zertifikat validieren	Optional. Validiert das Zertifikat und importiert das vCenter-Stammzertifikat in den Speicher für vertrauenswürdige Zertifikate der Cisco ISE. Überprüfen Sie während des Imports auch Vertrauenswürdig für die Authentifizierung von Cisco Services. Für Produktionsumgebungen wird die Zertifikatsvalidierung empfohlen.



Seite "Workload-Verbindung erstellen" mit den ausgefüllten Detailfeldern für die vCenter-Verbindung und aktiviertem Kontrollkästchen "vCenter-Zertifikat validieren"

In diesem Bild wird im Feld Benutzer ein Platzhalter angezeigt. Geben Sie die

Anmeldeinformationen für Ihre Umgebung ein.

Anmerkung: Die Cisco ISE validiert die von Ihnen eingegebenen Informationen. Wenn Details falsch sind, gibt die Cisco ISE den Fehler Verbindung testen fehlgeschlagen zurück.

---

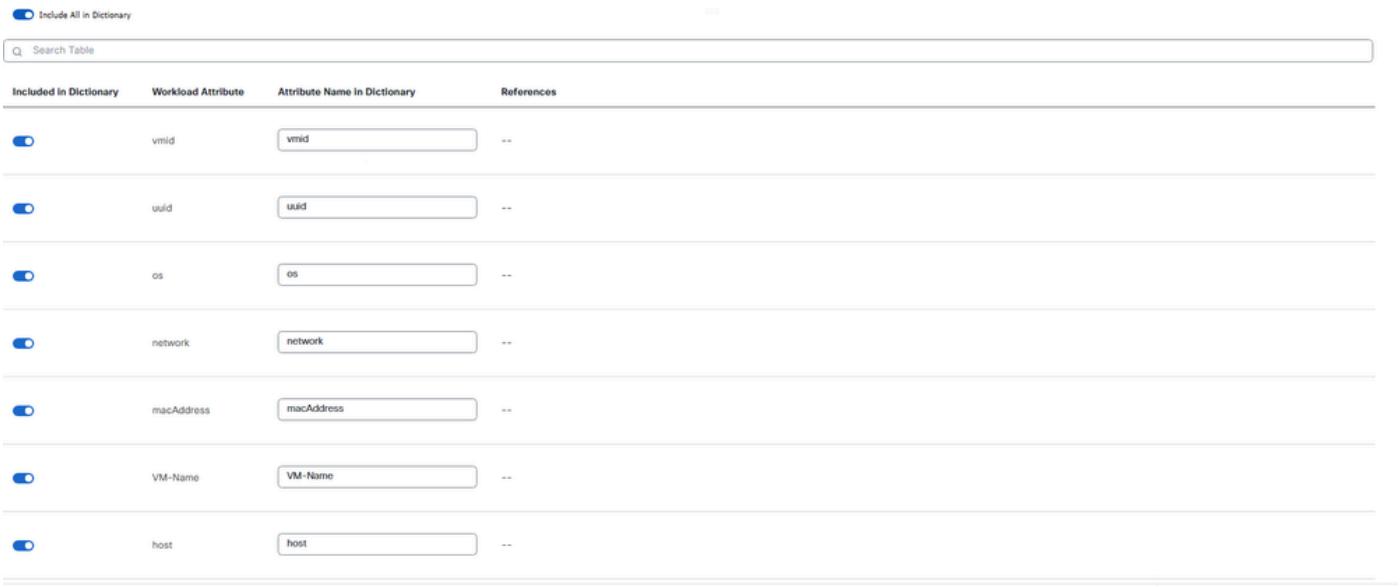
7. Klicken Sie auf Next (Weiter). Die Cisco ISE testet die Verbindung und bestätigt das Ergebnis mit der Meldung Die Verbindung wurde getestet.

Erfolgsbenachrichtigung, die bestätigt, dass die Testverbindung mit vCenter erfolgreich hergestellt wurde

Erfolgsbenachrichtigung, die bestätigt, dass die Testverbindung mit vCenter erfolgreich hergestellt wurde

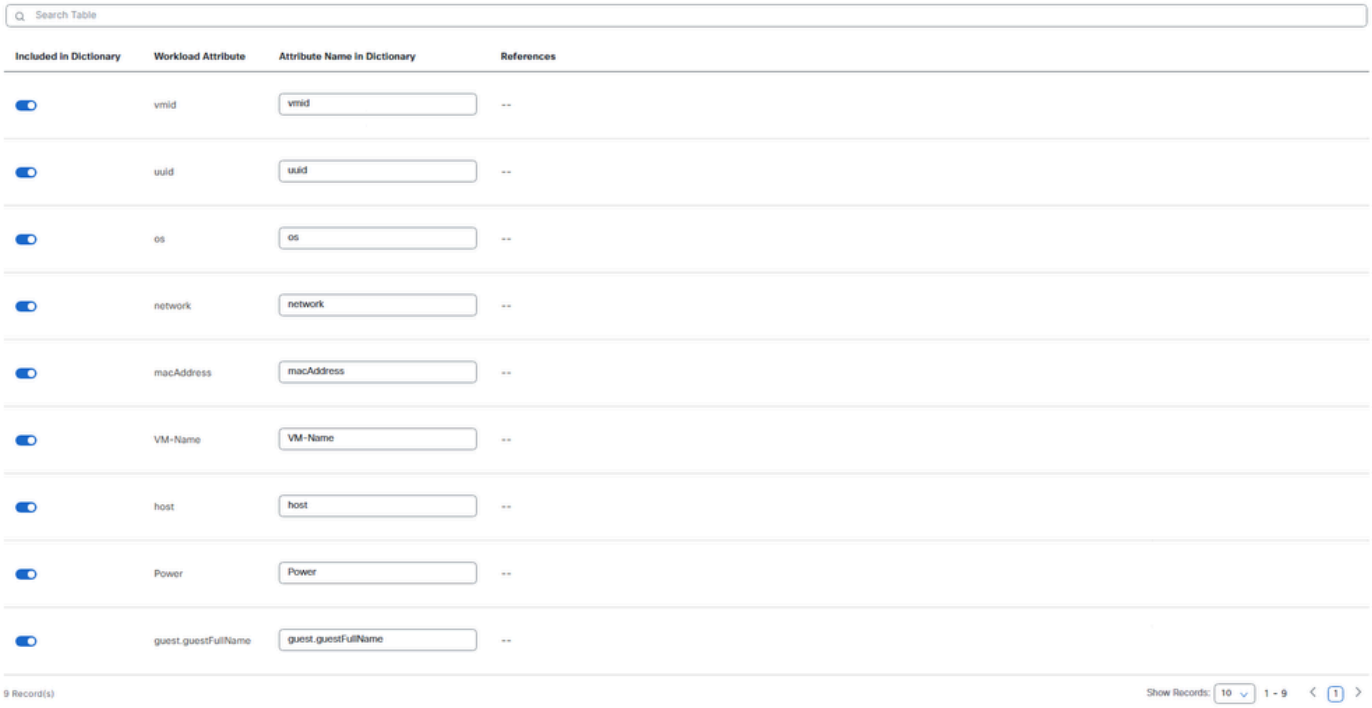
8. Wählen Sie auf der Seite Manage Attributes (Attribute verwalten) die vCenter-Attribute aus, die dem Cisco ISE-Wörterbuch hinzugefügt werden sollen. Stellen Sie in diesem Beispiel sicher, dass das os-Attribut enthalten ist. Klicken Sie dann auf Weiter.

- Um alle gelernten Attribute gleichzeitig einzubeziehen, aktivieren Sie den Umschalter Alle in Wörterbuch einschließen.
- Um ein Attribut umzubenennen, bearbeiten Sie den Attributnamen im Feld Dictionary.
- Es muss mindestens ein Attribut hinzugefügt werden, bevor Sie fortfahren können.
- Attributnamen, die Sonderzeichen wie ^, =, ", \, |, :, [oder] sind ungültig und können nicht hinzugefügt werden.



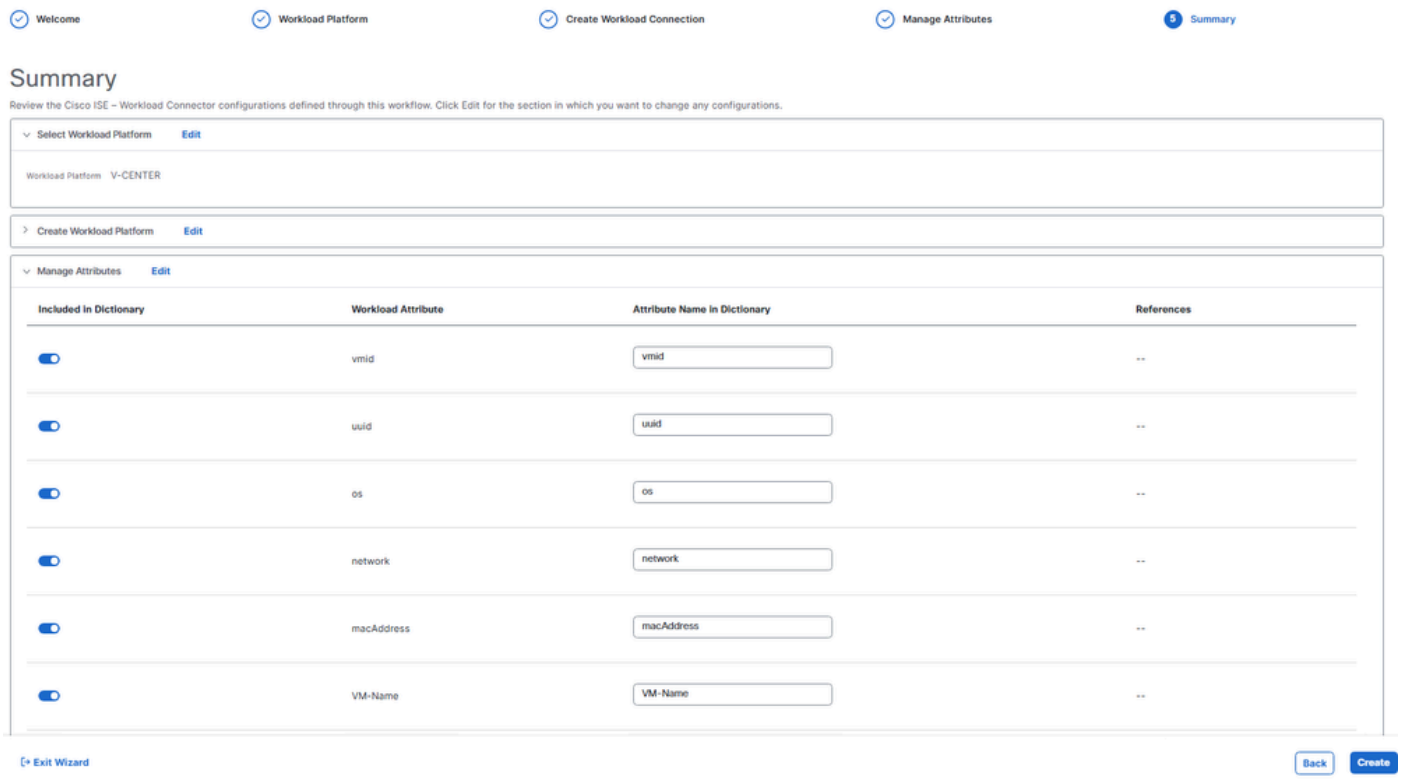
Seite "Attribute verwalten" mit aktiviertem Umschalter "Alle in Wörterbuch einschließen" und aufgeführter vCenter-Attribute

Führen Sie in der Liste einen Bildlauf durch, um alle Attribute zu überprüfen, die die Verbindung von vCenter erhalten hat, z. B. vmid, uid, os, network, macAddress, VM-Name, host, Power und guest.guestFullName.



Seite "Manage Attributes" (Attribute verwalten), um die vollständige Liste der gelernten vCenter-Attribute und die Anzahl der Datensätze anzuzeigen

9. Überprüfen Sie auf der Seite Summary (Übersicht) die Konfiguration. Klicken Sie neben einem Abschnitt auf Bearbeiten, um dessen Werte zu ändern.



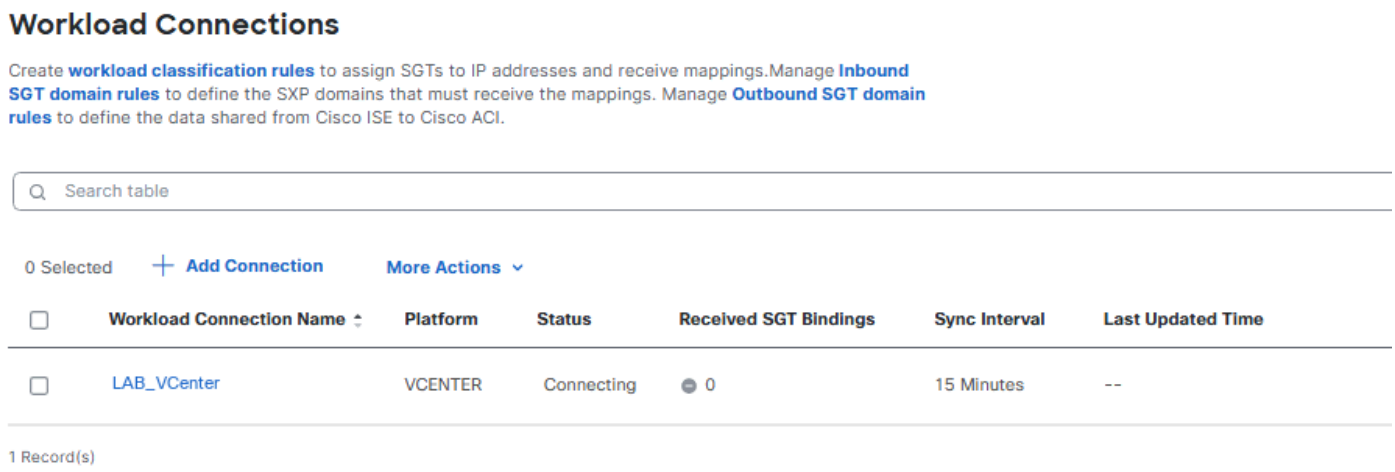
Übersichtsseite mit der ausgewählten V-CENTER-Workload-Plattform und den im Wörterbuch enthaltenen Attributen

10. Klicken Sie auf Erstellen. Cisco ISE bestätigt das Ergebnis, indem die Meldung Connection successfully created (Verbindung erfolgreich hergestellt) angezeigt wird.

Erfolgsbenachrichtigung zur Bestätigung, dass die Arbeitslastverbindung hergestellt wurde

Der neue vCenter-Connector wird auf der Seite Workload Connections (Workload-Verbindungen) angezeigt. Der Status lautet "Connecting" (Verbindung wird hergestellt), während die Cisco ISE

die Sitzung mit vCenter herstellt.



Seite "Workload Connections" (Workload-Verbindungen), auf der der neue vCenter-Connector im Status "Connecting" aufgeführt ist

Schritt 2: Hinzufügen von vCenter-Attributen zum Dictionary (optional)

Führen Sie diesen Schritt nur aus, wenn Sie ein benutzerdefiniertes Attribut hinzufügen möchten. Die Attribute, die Sie während des Schritts Attribute verwalten auswählen, werden dem vCenter-Wörterbuch automatisch hinzugefügt, sodass die Integration hier ohne Aktion funktioniert. Wörterbuchattribute können auch jederzeit nach dem Herstellen der Verbindung verwaltet werden:

1. Wählen Sie Work Centers > TrustSec > Integrations > Workload Connectors aus.
2. Klicken Sie auf Attributes Dictionary.
3. Klicken Sie auf Attribut hinzufügen.
4. Aktivieren Sie den Umschalter In Wörterbuch einschließen.
5. Geben Sie im Feld Workload-Attribut den Attributnamen ein, z. B. os.
6. Geben Sie im Feld Attributname in Dictionary den Namen ein, der angezeigt werden soll.
7. Klicken Sie auf Speichern.

Beachten Sie dieses Wörterbuchverhalten:

- Pro Verbindungstyp wird ein Wörterbuch erstellt. Alle vCenter-Connectors verwenden gemeinsam ein vCenter-Dictionary.
- Attribute werden nicht automatisch entfernt, wenn eine Verbindung gelöscht wird. Jedes

Attribut, das nicht verwendet wird, kann manuell gelöscht werden.

- Attribute können aus dem Anbieter importiert werden, und Attribute, die im Anbieter nicht vorhanden sind, können manuell hinzugefügt werden.

Schritt 3: Klassifizieren von Workloads in SGTs

Workload-Klassifizierungsregeln evaluieren Workload-Attribute, einschließlich der importierten vCenter-Tags, und weisen SGTs zu. Dieser Schritt liefert den Segmentierungswert der Integration.

Die SGT-Zuweisung verhält sich wie in den folgenden Artikeln beschrieben:

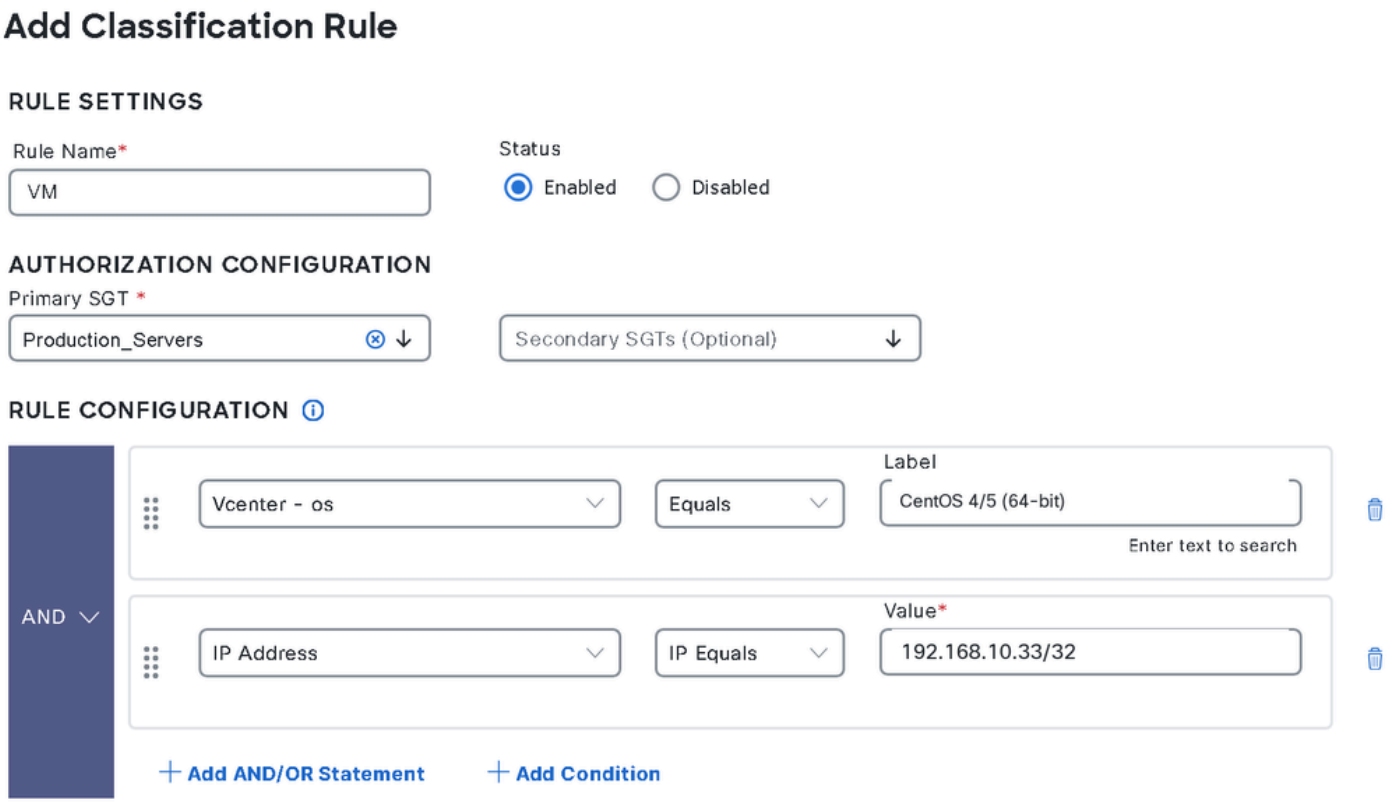
- Das primäre SGT wird im pxGrid-Sitzungsthema als Sicherheitsgruppe markiert und zum Veröffentlichen von IP-zu-SGT-Zuordnungen über SXP verwendet.
- Sekundäre SGTs sind im pxGrid-Sitzungsthema als geordnetes Array mit dem Namen Sekundäre Sicherheitsgruppen enthalten.
- Stimmen mehrere Regeln überein und weisen mehrere primäre SGTs zu, wird nur das erste zugewiesene SGT als primär behandelt. Die verbleibenden SGTs werden sekundär.

So erstellen Sie eine Klassifizierungsregel für dieses Beispiel:

1. Wählen Sie Work Centers > TrustSec > Integrations > Workload Classification aus.
2. Klicken Sie auf Klassifizierungsregel hinzufügen.
3. Geben Sie im Bereich RULE SETTINGS (REGELEINSTELLUNGEN) einen Regelnamen ein, und setzen Sie Status auf Enabled (Aktiviert).
4. Wählen Sie im Bereich AUTORISIERUNGSKONFIGURATION in der Dropdown-Liste Primäres SGT das von der Regel zugewiesene SGT aus, z. B. [SGT_NAME]. In diesem Beispiel wird das Production_Servers-SGT zugewiesen.
5. Wählen Sie optional aus der Dropdown-Liste Sekundäre SGTs (optional) ein oder mehrere sekundäre SGTs aus.
6. Erstellen Sie im Bereich RULE CONFIGURATION (Regelkonfiguration) die Übereinstimmungsbedingung. Wählen Sie in der Dropdown-Liste ein importiertes vCenter-Attribut aus, z. B. Vcenter - os, wählen Sie den Operator Equals, und geben Sie den entsprechenden Wert ein. Dieses Beispiel entspricht CentOS 4/5 (64-Bit).
7. Um die Regel weiter einzugrenzen, klicken Sie auf Bedingung hinzufügen, und kombinieren Sie die Bedingungen mit AND oder OR. In diesem Beispiel wird eine IP Address-Bedingung hinzugefügt, die den IP Equals-Operator verwendet, um die Regel auf die einzelne Host-Adresse 192.168.10.33/32 zu beschränken.

8. Klicken Sie ggf. auf Vorschau, um die SGT-Details und die Workloads zu überprüfen, denen die Regel entspricht.
9. Klicken Sie auf Hinzufügen.

⚠ Vorsicht: Der Equals-Operator erfordert den vollständigen Attributwert. vCenter meldet das Gastbetriebssystem als vollständige beschreibende Zeichenfolge wie CentOS 4/5 (64-Bit) und nicht als Kurzname wie CentOS. Eine Regel, die Equals CentOS anhand dieses Werts testet, stimmt nie überein und schlägt im Hintergrund fehl: Der Connector importiert weiterhin Workloads, aber es wurde kein SGT zugewiesen. Bestätigen Sie den genauen Wert in der Kontexttransparenz, bevor Sie die Regel erstellen, wie im Abschnitt Überprüfen beschrieben, oder verwenden Sie einen Operator wie Enthält, wenn Sie mit einer Familie von Gastbetriebssystemen übereinstimmen möchten.



Seite "Klassifizierungsregel hinzufügen", auf der das primäre SGT "Production_Servers" zugewiesen wird, wenn das Attribut "vCenter os" CentOS 4/5 (64-Bit) und die IP-Adresse 192.168.10.33/32 entspricht

Wiederholen Sie diese Schritte für jede zusätzliche Gruppe von Workloads, die Sie klassifizieren möchten, und weisen Sie jeder Regel ein anderes primäres SGT zu.

Beachten Sie dieses Regelverhalten:

- Regeln können per Drag & Drop neu sortiert werden. Die Reihenfolge bestimmt die Priorität.
- Eine neue Regel oder eine doppelte Regel kann vor oder nach einer bestehenden Regel eingefügt werden.
- Die Standardklassifizierungsregel befindet sich immer am Ende der Liste, ist standardmäßig deaktiviert und dem unbekannten primären SGTs zugeordnet.
- Verwenden Sie die Option Vorschau, um SGT-Details und Zuordnungsregeln vor dem Speichern zu überprüfen.

Schritt 4: Weiterleitungsbindungen mit eingehenden und ausgehenden SGT-Domänenregeln

SGT-Domänen steuern, welche Teile des Netzwerks bestimmte SGT-Bindungen erhalten. Wenn keine eingehenden Regeln definiert sind, werden die von den Workload-Connectors empfangenen Bindungen an die Standard-SGT-Domäne gesendet.

Hinzufügen einer eingehenden SGT-Domänenregel:

1. Wählen Sie Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules aus.
2. Klicken Sie auf der Registerkarte "Inbound SGT Domain Rules" (Eingehende SGT-Domänenregeln) auf Add Inbound Rule (Eingehende Regel hinzufügen).
3. Geben Sie im Bereich Regeleinstellungen einen Regelnamen ein.
4. Klicken Sie auf Aktiviert.
5. Wählen Sie in der Dropdown-Liste Destination (Ziel) die SGT-Domänen aus, die die Bindungen empfangen müssen. Um eine Domäne hinzuzufügen, verwenden Sie Create SGT Domain (SGT-Domäne erstellen).
6. Erstellen Sie im Bereich Rule Configuration (Regelkonfiguration) die Bedingung anhand von Attributen wie SGT Name, Quelle, IP-Adresse oder einem beliebigen vCenter-Attribut, das dem Wörterbuch hinzugefügt wurde, z. B. os. Kombinieren Sie die Bedingungen je nach Bedarf mit AND und OR.
7. Klicken Sie auf Hinzufügen und dann auf Speichern.

Fügen Sie eine ausgehende SGT-Domänenregel hinzu:

1. Öffnen Sie auf derselben Seite die Registerkarte Outbound SGT Domain Rules (Ausgehende SGT-Domänenregeln), und klicken Sie auf Add Outbound Rule (Ausgehende Regel hinzufügen).
2. Geben Sie einen Regelnamen ein, und klicken Sie auf Aktiviert.

3. Wählen Sie in der Dropdown-Liste Destination (Ziel) die Ziele aus, an die die SGTs gesendet werden sollen.
4. Erstellen Sie im Bereich Rule Configuration (Regelkonfiguration) die Bedingung aus SGT-Domänen, SGT-Name oder IP-Adresse.
5. Weisen Sie ggf. im Bereich "Vertragskonfiguration" den freigegebenen Sicherheitsgruppen "Genutzte" und "Bereitgestellte" Verträge zu.
6. Klicken Sie auf Hinzufügen und dann auf Speichern.

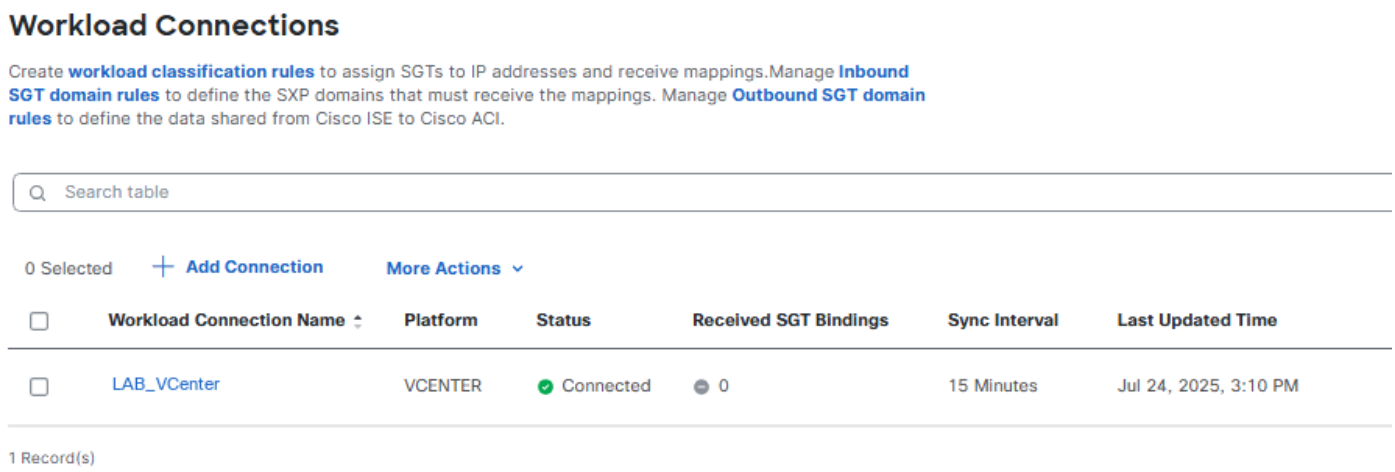
Verwenden Sie die Option Vorschau, um die übereinstimmenden IP-SGT-Bindungen zu überprüfen, während Sie eingehende und ausgehende Regeln hinzufügen oder bearbeiten.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verbindungsstatus überprüfen

Wählen Sie Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections aus, und bestätigen Sie, dass die vCenter-Verbindung mit dem Status Connected (Verbunden) aufgeführt ist. Auf dieser Seite können Sie eine Verbindung auch erneut herstellen, aussetzen oder löschen.



Seite "Workload Connections" (Workload-Verbindungen), auf der der vCenter-Connector mit dem Status "Connected", der Anzahl der empfangenen SGT-Bindungen, dem Synchronisierungsintervall und der letzten aktualisierten Zeit angezeigt wird

Die Spalte Empfangene SGT-Bindungen lautet in diesem Bild 0, da die Erfassung ausgeführt wurde, bevor eine Klassifizierungsregel einer Arbeitslast entsprach. Der Status "Verbunden" und die Anzahl der Bindungen Null bedeuten, dass die Cisco ISE vCenter erfolgreich erreicht hat, aber noch keinem SGT ein solches zugewiesen hat. Wenn eine Regel übereinstimmt, wird in dieser Spalte die Anzahl der von der Cisco ISE abgeleiteten Bindungen angezeigt.

Sicherheitsgruppen überprüfen

Wählen Sie Work Centers > TrustSec > Components > Security Groups aus, und bestätigen Sie, dass die erwarteten SGTs vorhanden sind. Bestätigen Sie in diesem Beispiel, dass das Production_Servers-SGT vorhanden ist.

Überprüfen der IP-SGT-Bindungen

Wählen Sie Work Centers > TrustSec > SXP > SGT Bindings aus, und stellen Sie sicher, dass die Workload-IP-Adressen an die richtigen SGTs mit der richtigen Quelle und der richtigen angewendeten Klassifizierungsregel gebunden sind.

Überprüfen der Workload-Live-Sitzungen

Wählen Sie Operations > Workloads > Live Session aus, um die Seite Workload Live Sessions zu öffnen. Live-Sitzungen können nur auf dem primären Policy Administration Node (PAN) angezeigt werden. Auf dieser Seite können Sitzungen nach Verbindungstyp gefiltert, Spalten angezeigt, ausgeblendet und neu angeordnet, Ergebnisse sortiert, Filter gespeichert und Daten im CSV- oder PDF-Format exportiert werden.

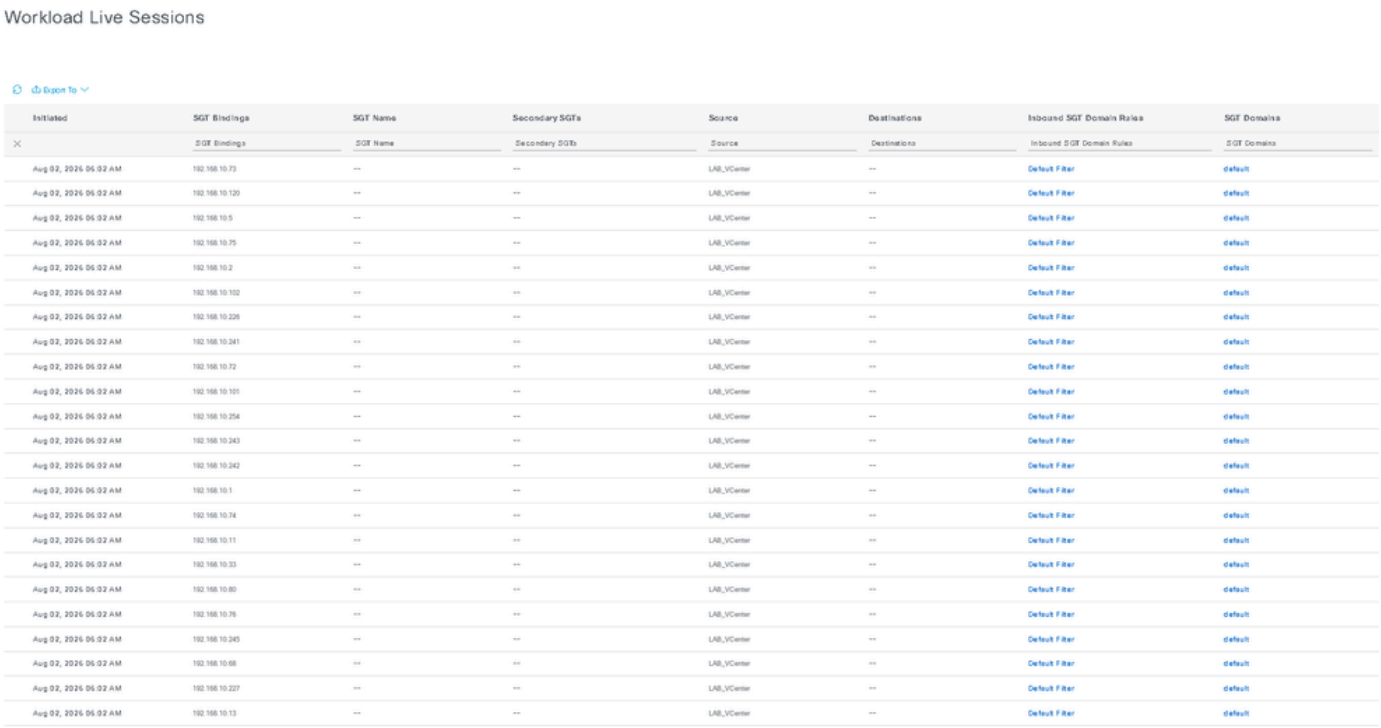


Tabelle "Workload Live Sessions" mit einer Zeile pro abgefragter Workload, mit dem initiierten Zeitstempel, der IP-Adresse der SGT-Bindungen, dem leeren SGT-Namen, den sekundären SGTs und den Spalten für Ziele, dem Quellverbindungsnamen LAB_VCenter und den Links "Inbound SGT Domain Rules and SGT Domains" mit dem Standardfilter und der Standardeinstellung.

Anmerkung: Diese Erfassung wird auf die Spalten zugeschnitten, die in diesem Beispiel Daten enthalten. Die Spalten "Outbound SGT Domain Rules" (Ausgehende SGT-Domänenregeln) und "Workload Classification Rules" (Workload-Klassifizierungsregeln) werden rechts neben dem sichtbaren Bereich angezeigt und sind in jeder Zeile leer. Gleiches gilt für die darüber hinausgehenden ACI-spezifischen Spalten. Diese Seite wurde in einer späteren Übungssitzung erfasst als die Konfigurationsseiten der Connectors, sodass ihre initiierten Zeitstempel nicht mit der letzten aktualisierten Zeit übereinstimmen, die zuvor auf der Seite "Workload-Verbindungen" angezeigt wurde.

Jede Zeile steht für eine Workload, die die Cisco ISE von einem Connector erhalten hat. Verwenden Sie die folgenden Spalten, um die Integration zu bestätigen:

Spalte	Was sie bestätigt
Initiiert	Zeitpunkt, zu dem die Cisco ISE von der Sitzung erfuhr Aktuelle Zeitstempel bestätigen, dass der Connector eine Abfrage durchführt.
SGT-Bindungen	Die Workload-IP-Adresse, die Cisco ISE von vCenter

Spalte	Was sie bestätigt
	erhalten hat.
Quelle	Die Arbeitslastverbindung, von der die Sitzung gemeldet wurde. Gibt an, von welchem Connector die Daten stammen.
Eingehende SGT-Domänenregeln und SGT-Domänen	Die Domänenregel und die SGT-Domäne, die auf die Sitzung angewendet wurden. Klicken Sie auf einen Link, um die zugeordnete Regel anzuzeigen.
SGT-Name, sekundäre SGTs und Workload-Klassifizierungsregeln	Die dem Workload zugewiesenen SGTs und die Regel, die ihnen zugewiesen hat. Diese Spalten bleiben für Workloads leer, die nicht mit einer Klassifizierungsregel übereinstimmen.

Verwenden Sie die Steuerelemente Aktualisieren, Anzeigen und Innerhalb rechts oben auf der Seite rechts neben dem zugeschnittenen Bereich, um das Aktualisierungsintervall, die Datensatzanzahl und das Zeitfenster festzulegen.

In diesem Abbild wird die Spalte SGT-Bindungen vollständig ausgefüllt, während SGT-Name und sekundäre SGTs in jeder Zeile leer sind, da die Erfassung vor dem Abgleich einer Klassifizierungsregel durchgeführt wurde. Die Spalte Workload-Klassifizierungsregeln, die sich außerhalb des zugeschnittenen Bereichs befindet, ist aus demselben Grund leer. Diese Kombination ist an sich schon eine nützliche Diagnose: Es bestätigt, dass der Connector Workloads korrekt aus vCenter abruft und dass das Problem eher in den Regelbedingungen als in der Verbindung liegt. Kehren Sie dann zu Schritt 3 zurück, und vergleichen Sie die Übereinstimmungswerte mit den Attributwerten, die von Context Visibility gemeldet werden, wie in diesem Schritt unter Vorsicht beschrieben.

Überprüfung der Workload-Transparenz in der Kontexttransparenz

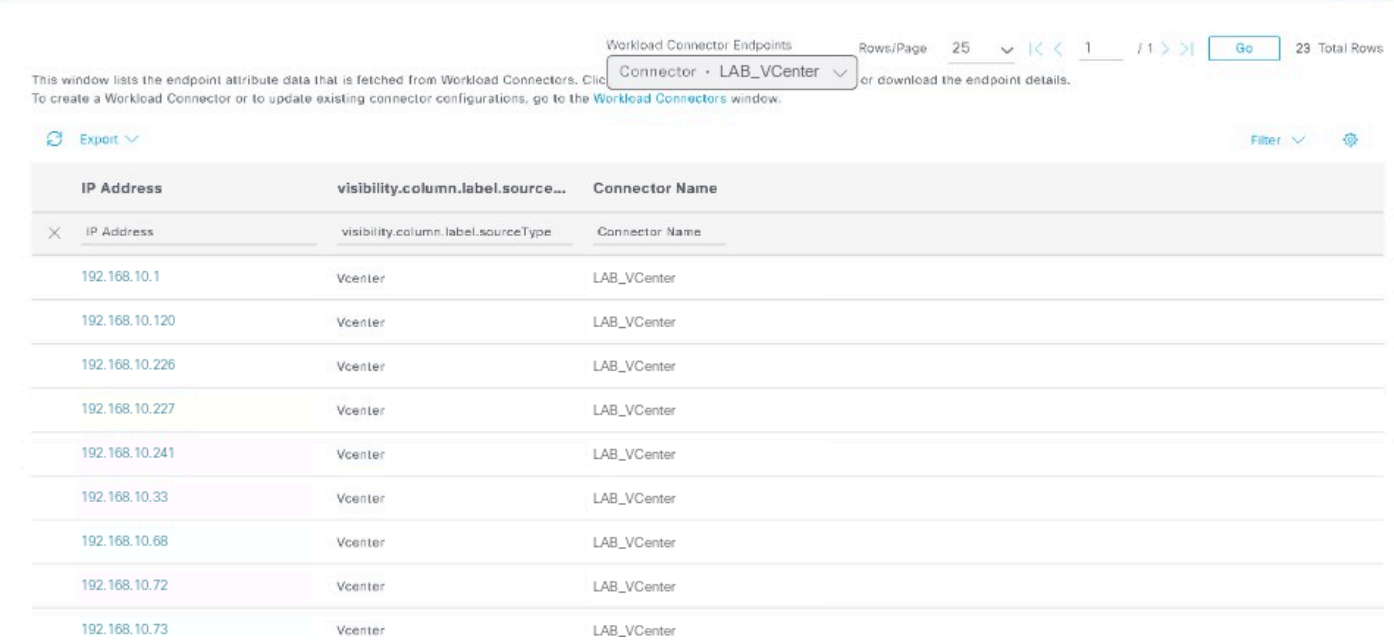
⚠ Versionsanforderung: Das Workload Connector Endpoints-Dashboard ist ab Cisco ISE 3.5 Patch 3 verfügbar. Verwenden Sie auf der Cisco ISE 3.4 die Seite Workload Live Sessions, die im vorherigen Abschnitt beschrieben wurde.

Die Cisco ISE bietet ein dediziertes Workload Connector-Endgeräte-Dashboard mit Context Visibility. Die Lösung erfasst, analysiert und meldet die Endgeräteattributdaten, die von Workload-Konnektoren erfasst wurden, in einer einzigen, filterbaren Ansicht.

So öffnen Sie die Ansicht:

1. Wählen Sie in der Cisco ISE-GUI Context Visibility > Endpoints (Kontexttransparenz > Endpunkte).
2. Öffnen Sie die Registerkarte Workload Connector-Endpunkte. Wenn die Registerkarte im Registerkartenstreifen nicht sichtbar ist, klicken Sie auf Mehr.
3. Wählen Sie aus der Dropdown-Liste Connector (Connector) die Workload-Verbindung aus, deren Endpunkte Sie überprüfen möchten.

Das Fenster listet die Endpunktattributdaten auf, die von den Workload-Konnektoren abgerufen werden. Jede Zeile identifiziert einen Endpunkt anhand der IP-Adresse, des Quelltyps und des Connectornamens.



Workload Connector-Endpunkte werden in der Ansicht unter "Context Visibility" nach IP-Adresse, Quelltyp und Connectorname aufgelistet, wobei die Connector-Dropdown-Liste auf LAB_VCenter, die Exportoption, die Zeilen-/Paging- und Paginierungssteuerelemente und eine Anzahl von insgesamt 23 Zeilen festgelegt ist.

In dieser Ansicht können Sie:

- Filtern Sie die Liste. Verwenden Sie die Filterzeile unter den Spaltenüberschriften, um die Ergebnisse nach IP-Adresse, Quelltyp oder Konnektorname einzugrenzen. Filter sind additiv, sodass jeder angewendete Wert die Ergebnismenge weiter verfeinert.
- Blättern Sie durch die Ergebnisse. Verwenden Sie das Rows/Page-Steuerelement und die Paginierungspfeile, um die Seitengröße zu ändern und zwischen den Seiten zu wechseln. Die

Gesamtzahl der Endpunkte wird rechts neben den Pfeilen angezeigt, hier als 23 Gesamtzeilen.

- Exportieren der Daten Klicken Sie auf Exportieren, um die aufgelisteten Endpunktdaten herunterzuladen.
- Überprüfen Sie einen Endpunkt. Klicken Sie auf die IP-Adresse eines Endpunkts, um den Folienbereich Details zu öffnen.

Im Bereich Details werden alle Attribute aufgeführt, die die Cisco ISE für den ausgewählten Endpunkt enthält. Klicken Sie auf Herunterladen, um die Attributdetails zu speichern, oder klicken Sie auf Abbrechen, um den Bereich zu schließen.

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

Detaillierter Einblendbereich für einen ausgewählten Workload-Endpunkt mit dem Titel Details über dem Konnektornamen und der Endpunktadresse, mit der ATTRIBUTES-Liste der vCenter-Eigenschaften, die von der Cisco ISE für das virtuelle System erfasst wurden, und den Steuerelementen Abbrechen und Herunterladen

Der Bereich ist durch den Namen der Workload-Verbindung und die Endpunktadresse gekennzeichnet (hier als LAB_VCenter_192.168.10.1 dargestellt). Für einen vCenter-Workload-Endpunkt umfassen die Attribute die Eigenschaften der virtuellen Maschine, die von vCenter bezogen wurden, wie Power, VM-Name, Host, macAddress, Netzwerk, os, uuid, vmid und vmtype. mit den Connector-Metadaten CorrelationId, Source, ipAddress, connectorType und SourceType. Alle benutzerdefinierten vCenter-Tags, die Sie dem Wörterbuch hinzugefügt haben, werden auch hier angezeigt.

Dieser Bereich ist die maßgebliche Quelle für die Werte, mit denen die Klassifizierungsregeln übereinstimmen müssen. Wenn Sie diesen Bereich zuerst überprüfen, wird der häufigste Fehler in diesem Workflow verhindert. In diesem Bild liest os CentOS 4/5 (64-Bit), die vollständige Zeichenfolge, die eine Equals-Bedingung reproduzieren muss. Lesen Sie den Wert hier, bevor Sie die Regel in Schritt 3 schreiben, anstatt eine kurze Form wie CentOS anzunehmen.

Anmerkung: Es werden maximal 50 Attribute für jeden Endpunkt angezeigt.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Häufige Probleme

Symptom	Wahrscheinliche Ursache	Aktion
Testverbindung während Verbindungseinrichtung fehlgeschlagen	Mindestens eine Verbindungsdetails ist falsch, oder eine erforderliche Komponente ist nicht erfüllt.	Überprüfen Sie die FQDN- oder IP-Adresse, und stellen Sie sicher, dass sie mit dem Zertifikat-SAN übereinstimmt. Überprüfen Sie den Benutzernamen und das

Symptom	Wahrscheinliche Ursache	Aktion
		Kennwort, überprüfen Sie die Zertifikatvalidierungseinstellung, und stellen Sie sicher, dass die Voraussetzungen für die Proxy-Umgehung und die Zeitsynchronisierung erfüllt sind.
Connector wird erstellt, aber keine Daten werden importiert	Die Cisco ISE kann nicht auf public.ecr.aws zugreifen.	Bestätigen Sie, dass der Proxy oder die Firewall HTTPS-Datenverkehr über den TCP-Port 443 an diese URL zulässt.
Workloads werden importiert, es wird jedoch kein SGT zugewiesen, und die empfangenen SGT-Bindungen bleiben bei 0.	Eine Klassifizierungsregelbedingung stimmt nicht mit dem tatsächlichen Attributwert überein. Eine Equals-Bedingung, die mit einem Teilwert getestet wurde, wie CentOS anstelle von CentOS 4/5 (64-Bit), ist die häufigste Ursache.	Öffnen Sie den Bereich Details in der Kontexttransparenz, lesen Sie den genauen Attributwert, und korrigieren Sie die Regelbedingung, oder ändern Sie den Operator zu Enthält. Dieser Fehler ist stumm: es wird kein Alarm ausgelöst, da der Steckverbinder selbst fehlerfrei ist.
Die Verbindung wird in den Zustand Suspended (Ausgesetzt) versetzt	Alle der Verbindung zugeordneten SGTs wurden gelöscht.	Erstellen Sie die erforderlichen SGTs neu, und stellen Sie die Verbindung wieder her. Die zugehörigen SXP-Bindungen und MnT-Sitzungsdaten werden entfernt, während die Verbindung unterbrochen wird.
Nach einem PSN-Neustart fehlen die Verbindungsdetails.	Sitzungsdaten wurden nicht neu aufgefüllt	Die Verbindung unterbrechen und dann erneut verbinden.

Debug-Protokolle aktivieren

Legen Sie den Schweregrad des Debug-Protokolls für die Workload Connector-Komponente auf

den PAN-, SXP- und pxGrid-Knoten über Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration auf DEBUG fest.

Diese Protokolldateien sind in /opt/CSCOcpm/logs verfügbar:

Protokolldatei	Inhalt
Workloads.log	Workload Connector-Vorgänge.
workload-conn/*.log	Protokolle pro Verbindung.
api-service.log	API-Service-Aktivität.
ise-psc.log	Cisco ISE Policy Service-Aktivität.
pxgriddirect-service.log	pxGrid Direct-Serviceaktivität.
sxp_appserver/sxp.log	SXP-Bindungsverteilung.

Alarme

Die Cisco ISE erzeugt diese Alarme für vCenter und andere Cloud Connectors:

Alarm	Wird ausgelöst, wenn
Erstellung/Verbindung der Workload-Verbindung fehlgeschlagen	Die Connectorerstellung schlägt nach einem Ereignis wie einer Wiederherstellung, einer Werbemaßnahme, einem HA-Ereignis oder einem Upgrade fehl.
Löschen der Arbeitslastverbindung fehlgeschlagen	Löschen des Connectors fehlgeschlagen.
Fehler beim Arbeitslastverbindungsdienst	Ein weiterer damit zusammenhängender Dienstfehler tritt auf.

Zugehörige Informationen

- Cisco ISE Common Policy und Workload Connectors
- Erforderliche Internet-URLs für die Cisco ISE
- Cisco ISE 3.5 Administratorleitfaden
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.