

ISE Workload Connector-integratie configureren met VMware vCenter

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Cisco ISE](#)

[VMware vCenter](#)

[connectiviteit](#)

[getuigschriften](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[sleutelbegrippen](#)

[Gebruikte plaatsaanduidingen](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 1. De vCenter-werklastverbinding toevoegen](#)

[Stap 2. vCenter-kenmerken aan het woordenboek toevoegen \(optioneel\)](#)

[Stap 3. Werkbelastingen classificeren in SGT's](#)

[Stap 4. Routebindingen met inkomende en uitgaande SGT-domeinregels](#)

[Verifiëren](#)

[De verbindingstatus controleren](#)

[De beveiligingsgroepen controleren](#)

[Controleer de IP-SGT-bindingen](#)

[De werkbelasting tijdens live sessies controleren](#)

[Zichtbaarheid van werkbelasting in context controleren](#)

[Problemen oplossen](#)

[Veelvoorkomende problemen](#)

[Foutopsporingslogboeken inschakelen](#)

[alarm](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco ISE Workload Connector for VMware vCenter configureert om de context van de werklast te importeren en groepsgebaseerde segmentatie af te

dwingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE-beheer
- VMware vCenter-beheer
- Cisco TrustSec-concepten, waaronder Security Group Tags (SGT's), SGT Exchange Protocol (SXP) en pxGrid

Voordat u een vCenter-werklastverbinding toevoegt, moet u controleren of aan deze voorwaarden is voldaan.

Cisco ISE

- pxGrid is ingeschakeld op ten minste één knooppunt in de implementatie.
- SXP is ingeschakeld op ten minste één knooppunt in de implementatie.

VMware vCenter

- Er is een vCenter-account met alleen-lezen-machtiging beschikbaar. De connector voert alleen leesbewerkingen uit.
- De te importeren vCenter-kenmerken of -tags zijn geïdentificeerd. In dit document wordt het kenmerk os als voorbeeld gebruikt.

connectiviteit

- Een stabiele internetverbinding is beschikbaar voor Cisco ISE, omdat Cisco ISE public.ecr.aws kan bereiken, wat vereist is door de functie Workload Connector. Als een proxyserver of firewall zich in het pad bevindt, staat u HTTPS-verkeer (TCP-poort 443) toe tussen Cisco ISE en deze URL. Als deze URL onbereikbaar is, werkt de werklastconnector niet zoals bedoeld.
- Als een proxy wordt gebruikt voor internettoegang en vCenter on-premises wordt geïmplementeerd, configureert u een proxybypass voor het vCenter IP-adres.

getuigschriften

- Als certificaatvalidatie wordt gebruikt, moet het voor vCenter ingevoerde FQDN- of IP-adres overeenkomen met de alternatieve onderwerpsnaam (SAN) van het vCenter-eindpuntcertificaat.
- Het vCenter-basiscertificaat moet beschikbaar zijn voor import in de Cisco ISE Trusted Certificates-winkel.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine (ISE), versie 3.4, gebruikt voor de configuratie- en verificatieprocedures van de connector
- Cisco Identity Services Engine (ISE), versie 3.5 Patch 3, alleen gebruikt voor de zichtbaarheidsprocedure
- VMware vCenter Server 8.0 Update 3



Opmerking: het dashboard voor werklustconnectoreindpunten in Context Visibility vereist Cisco ISE 3.5-patch 3 of hoger, zodat de twee afbeeldingen in die sectie op die release zijn vastgelegd. Elke andere procedure en afbeelding in dit document is afkomstig van Cisco ISE 3.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Moderne datacenters zijn dynamisch. Virtuele machines (VM's) worden voortdurend gemaakt, verplaatst en met pensioen gegaan en hun IP-adressen veranderen mee. Beveiligingsbeleid dat afhankelijk is van statische IP-adressen of subnetten kan geen gelijke tred houden met deze snelheid van verandering, wat gaten laat in zowel handhaving als zichtbaarheid.

Cisco ISE pakt dit probleem aan via het Common Policy framework en de Workload Connectors. Een Workload Connector maakt een veilige verbinding met een datacenter of cloudplatform, importeert de context van de applicatieworkloads die daar worden uitgevoerd, normaliseert die

context in SGT's en deelt het resultaat met de rest van het netwerk, zodat het beleid ertegen kan worden geschreven.

vCenter beschrijft elke virtuele machine al aan de hand van een reeks kenmerken, zoals het gastbesturingssysteem, de poortgroep waaraan het wordt gekoppeld en de energiestatus. VMware-beheerders breiden die beschrijving uit met aangepaste tags die metagegevens bevatten, zoals omgeving, toepassingsniveau, eigenaar of bedrijfseenheid. De vCenter Workload Connector importeert beide en zet deze om in SGT's. Dit levert drie resultaten op:

- Beleid is gebaseerd op werkdruk. Wanneer een VM wordt verplaatst of opnieuw wordt geadresseerd, blijft de van het kenmerk afgeleide SGT bij, zodat segmentatie blijft werken zonder handmatige updates.
- Bestaande context wordt hergebruikt. Cisco ISE verbruikt de attributen en tags die vCenter al onderhoudt, dus er is geen nieuw classificatieschema vereist.
- De segmentatie is consistent. SGT's worden verspreid over het TrustSec-netwerk, dus hetzelfde beleid is van toepassing op elk handhavingspunt.

In dit document wordt één lopend voorbeeld gebruikt. Het os-attribuut dat vCenter rapporteert voor elke virtuele machine, die in dit lab CentOS 4/5 (64-bits) leest, wordt geïmporteerd in Cisco ISE en gecombineerd met een IP-adresvoorwaarde, zodat de overeenkomende werklasten automatisch in een Production_Servers-beveiligingsgroep worden geplaatst. Die werklasten worden vervolgens gesegmenteerd op groepslidmaatschap in plaats van handmatig bijgehouden IP-adressen. Dezelfde procedure is van toepassing op elk ander attribuut of aangepaste tag die vCenter blootlegt.

sleutelbegrippen



Opmerking: VMware ESXi ondersteunt geen tags. Daarom kan alleen vCenter worden geconfigureerd als een werklasterconnector. Standalone ESXi-hosts kunnen dat niet.

Begrip	Definitie
TrustSec	Cisco-technologie voor groepsgebaseerde segmentatie, waarbij beleid wordt geschreven tegen groepen in plaats van IP-adressen.
SGT (Security Group Tag)	Een tag die een groep vertegenwoordigt, zoals Production Workloads, en dient als basis voor beleidshandhaving.
SXP (SGT Exchange Protocol)	Het protocol wordt gebruikt om IP-naar-SGT-bindingen te distribueren naar handhavingsapparaten.

Begrip	Definitie
pxGrid	Het Cisco-platform werd gebruikt om context, zoals sessies en SGT's, te delen tussen Cisco ISE en andere systemen.
gemeenschappelijk beleid	Het Cisco ISE-framework dat verbinding maakt met datacenters en clouds, hun context normaliseert in SGT's en deze deelt over verschillende domeinen.
werklasterconnector	De Cisco ISE-component die verbinding maakt met vCenter, AWS, Azure, GCP of ACI en de werklastercontext importeert.

Gebruikte plaatsaanduidingen

Waarden tussen vierkante haakjes zijn plaatsaanduidingen. Vervang ze door de waarden die van toepassing zijn op uw omgeving.

plaatshouder	Beschrijving
[VCENTER_FQDN]	Volledig gekwalificeerde domeinnaam van de vCenter-server.
[VCENTER_IP_ADDRESS]	IP-adres van de vCenter-server.
[USERNAME]	Gebruikersnaam voor alleen-lezen vCenter-account.
[WACHTWOORD]	vCenter alleen-lezen accountwachtwoord.
[SGT_NAME]	Naam van de beveiligingsgroeptag die is toegewezen door een classificatieregel.
[VM_NAME]	Naam van een virtuele machine in vCenter.
[VM_UUID]	UUID van een virtuele machine in vCenter.
[VM_ID]	vCenter beheerde objectreferentie van een virtuele machine.
[HOST_ID]	vCenter beheerde objectreferentie van een ESXi-host.

plaatshouder	Beschrijving
[NETWORK_NAME]	Naam van de vCenter-poortgroep of -netwerk.

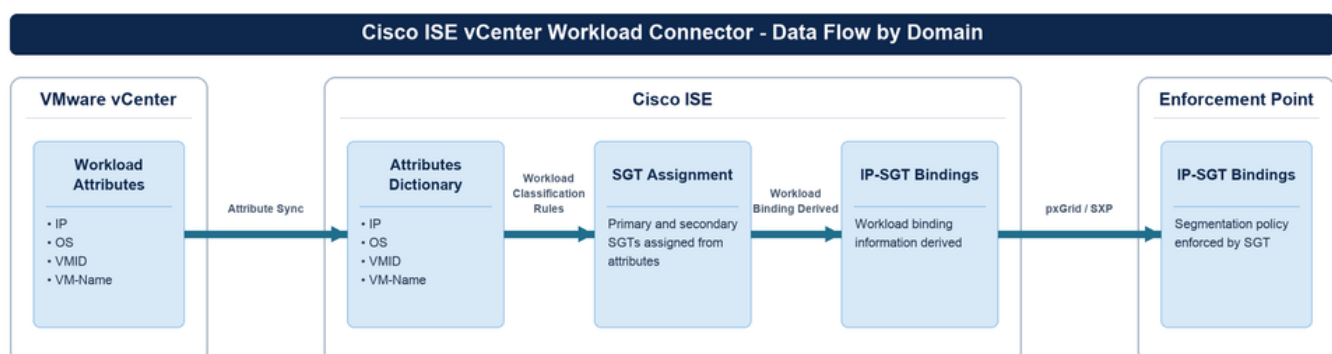
De afbeeldingen in dit document zijn afkomstig van een laboratorium dat de naam van de werklasterverbinding LAB_vCenter, het vCenter-adres 192.168.1.50 en het werklastsubnet 192.168.10.0/24 gebruikt. Vervang de namen en adressen die van toepassing zijn op uw omgeving.

Configureren

Netwerkdigram

De integratie transformeert vCenter-metagegevens in vijf fasen in afdwingbaar beleid:

1. De Cisco ISE vCenter Workload Connector leest de werklasterkenmerken en -tags van vCenter.
2. De geselecteerde attributen worden toegevoegd aan het Cisco ISE Attributes Dictionary zodat er in de regels naar kan worden verwezen.
3. De werklasterclassificatieregels evalueren deze kenmerken en wijzen een primaire SGT en optioneel een of meer secundaire SGT's toe aan elke werklaster.
4. Cisco ISE ontleent IP-naar-SGT-bindingen en publiceert ze via SXP en pxGrid. Inkomende en uitgaande SGT-domeinregels bepalen welke SGT-domeinen de bindingen ontvangen en waar ze worden gedeeld.
5. Handhavingpunten passen de SGT's toe om verkeer toe te staan of te weigeren.



Cisco ISE vCenter Workload Connector-gegevensstroom over drie domeinen. vCenter biedt werklasterkenmerken (IP, OS, VMID, VM-naam); Cisco ISE slaat deze op in het woordenboek met kenmerken, past werklasterclassificatieregels toe om

primaire en secundaire SGT's toe te wijzen en leidt IP-SGT-bindingen af; de bindingen worden gedeeld via pxGrid en SXP naar het handhavingspunt

Configuraties

Stap 1. De vCenter-werklastverbinding toevoegen

1. Klik in de Cisco ISE GUI op het menupictogram en kies Werkcentra > TrustSec > Integraties > Werklastverbindingen > Werklastverbindingen.
2. Klik op Verbinding toevoegen.

Workload Connections

Create **workload classification rules** to assign SGTs to IP addresses and receive mappings. Manage **Inbound SGT domain rules** to define the SXP domains that must receive the mappings. Manage **Outbound SGT domain rules** to define the data shared from Cisco ISE to Cisco ACI.



No Workload Connected

Add Connection

Pagina Verbindingen werklast zonder geconfigureerde verbindingen, met de knop Verbinding toevoegen

3. Klik op Laten we het doen.

1 Welcome 2 Workload Platform Configuration Summary

Welcome

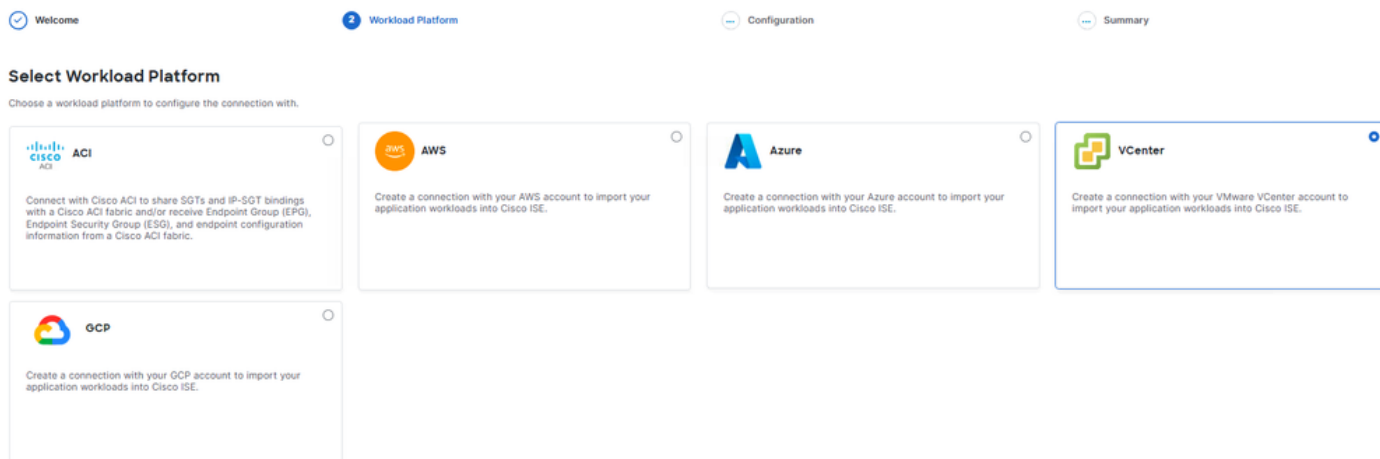
Use this wizard to set up a connection with a workload platform, and choose the attributes that you want to import into Cisco ISE. After the completion of this workflow, you can create workload classification rules, create ingress filters, and more, in Cisco ISE TrustSec pages.



Welkomspagina van de wizard Werklastverbinding met de stappen Welkom, Werklastplatform, Configuratie en Samenvatting van

de wizard

4. Kies op de pagina Selecteer werklastplatform vCenter en klik vervolgens op Volgende.



Selecteer de pagina voor het werklastplatform met de vCenter-optie die is geselecteerd voor de ACI-, AWS-, Azure- en GCP-platforms

5. Op de pagina Werklastverbinding maken controleert Cisco ISE of de Workload Connector-services actief zijn voordat deze verbindingsgegevens accepteert.

Als de services nog niet actief zijn, wordt op de pagina gemeld dat de Workload Connector-services niet actief zijn.

Create Workload Connection

Checking Prerequisites

Workload Connector Services are not running

Non-editable after creation

Description

Sync Interval*

15

Minutes

▼

FQDN or IP address*

Hint

User*

Password*

☐ Validate vCenter certificate. ⓘ

Een pagina voor werklasterbindingen maken waarin wordt gemeld dat de services voor werklasterbindingen niet worden uitgevoerd

Cisco ISE start de services vervolgens automatisch op en geeft de voortgang weer.

Create Workload Connection

Checking Prerequisites

Starting the services



Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes



FQDN or IP address*

[Hint](#)

User*

Password*

☐ Validate vCenter certificate. [?](#)

Pagina Werklastverbinding maken waarop de services voor werklastverbinding worden weergegeven

Wacht tot de pagina meldt dat Workload Connector Services actief is. De velden met verbindingdetails kunnen pas worden ingevuld nadat deze controle is geslaagd.

Create Workload Connection

Workload Connector Services are running

Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes

▼

FQDN or IP address*

Hint

User*

Password*

☐

Validate vCenter certificate.

Pagina Werklastverbinding maken om te bevestigen dat de Workload Connector-services actief zijn

6. Voer de verbindingsgegevens in:

Veld	Beschrijving
Naam werklstverbinding	Een unieke naam die letters, cijfers en onderstrepingen gebruikt. Maximaal 32 tekens, geen spaties. In dit voorbeeld wordt LAB_vCenter gebruikt.
Beschrijving	Een beschrijving van de verbinding.
synchronisatieinterval	Hoe vaak Cisco ISE gegevens uit vCenter vernieuwt. Geldig bereik is 60 seconden tot 7 dagen. De standaardtijd is 15 minuten. Kortere intervallen verversen gegevens vaker, maar kunnen de prestaties beïnvloeden.
FQDN- of IP-adres	De hostnaam of het IP-adres van vCenter, zoals [VCENTER_FQDN] of [VCENTER_IP_ADDRESS]. Deze waarde

Veld	Beschrijving
	moet overeenkomen met de alternatieve onderwerpnaam van het vCenter-eindpuntcertificaat.
Gebruiker	De gebruikersnaam van de vCenter-account, [USERNAME].
wachtwoord	Het vCenter-accountwachtwoord, [WACHTWOORD].
vCenter-certificaat valideren	Optioneel. Valideert het certificaat en importeert het vCenter-basiscertificaat in de Cisco ISE Trusted Certificates-winkel. Controleer tijdens het importeren ook Trust op verificatie van Cisco Services. Certificaatvalidatie wordt aanbevolen voor productieomgevingen.

Create Workload Connection

Workload Connector Services are running

Workload Connection Name*

LAB_VCenter

Non-editable after creation

Description

Sync Interval*

15

Minutes

FQDN or IP address*

192.168.1.50

Hint

User*

[USERNAME]

Password*

.....

Show

☒ Validate vCenter certificate. ⓘ

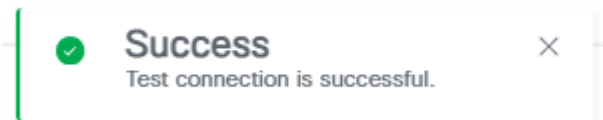
Pagina Werklastverbinding maken met de voltooide detailvelden voor vCenter-verbindingen en het selectievakje vCenter-certificaat valideren ingeschakeld

In deze afbeelding wordt in het veld Gebruiker een tijdelijke aanduiding weergegeven. Voer de referenties in die van toepassing zijn op uw omgeving.



Opmerking: Cisco ISE valideert de gegevens die u invoert. Als een detail onjuist is, geeft Cisco ISE de fout terug. De testverbinding is mislukt.

7. Klik op Next (Volgende). Cisco ISE test de verbinding en bevestigt dat het resultaat met het bericht Testverbinding succesvol is.



Succesmelding die bevestigt dat de testverbinding met vCenter succesvol is

Succesmelding die bevestigt dat de testverbinding met vCenter succesvol is

8. Op de pagina Attributen beheren kiest u de vCenter-attributen die u wilt toevoegen aan het Cisco ISE-woordenboek. Zorg er bijvoorbeeld voor dat het os-attribuut is opgenomen. Klik vervolgens op Volgende.

- Als u elk geleerd attribuut tegelijk wilt opnemen, schakelt u de schakeloptie Alles opnemen in woordenboek in.
- Als u de naam van een kenmerk wilt wijzigen, bewerkt u de naam van het kenmerk in het veld Woordenboek.
- Er moet ten minste één attribuut worden toegevoegd voordat u verder kunt gaan.
- Attribuutnamen die speciale tekens bevatten zoals ^, =, ", \, |, :, [, of] zijn ongeldig en kunnen niet worden toegevoegd.

☒ Include All in Dictionary

Q Search Table

Included in Dictionary	Workload Attribute	Attribute Name in Dictionary	References
☒	vmid	vmid	--
☒	uuid	uuid	--
☒	os	os	--
☒	network	network	--
☒	macAddress	macAddress	--
☒	VM-Name	VM-Name	--
☒	host	host	--

Pagina Kenmerken beheren met de schakelaar Alles opnemen in woordenboek ingeschakeld en de geleerde vCenter-kenmerken vermeld

Blader door de lijst om elk kenmerk te bekijken dat de verbinding heeft geleerd van vCenter, zoals vmid, uuid, os, netwerk, macAddress, VM-Name, host, Power en guest.guestFullName.

Q Search Table

Included in Dictionary	Workload Attribute	Attribute Name in Dictionary	References
☒	vmid	vmid	--
☒	uuid	uuid	--
☒	os	os	--
☒	network	network	--
☒	macAddress	macAddress	--
☒	VM-Name	VM-Name	--
☒	host	host	--
☒	Power	Power	--
☒	guest.guestFullName	guest.guestFullName	--

9 Record(s)

Show Records: 1 - 9 < 1 >

Op de pagina Eigenschappen beheren kunt u de volledige lijst met geleerde vCenter-kenmerken en het aantal records weergeven

9. Controleer de configuratie op de overzichtspagina. Klik naast een sectie op Bewerken om de waarden te wijzigen.

✓ Welcome

✓ Workload Platform

✓ Create Workload Connection

✓ Manage Attributes

5 Summary

Summary

Review the Cisco ISE – Workload Connector configurations defined through this workflow. Click Edit for the section in which you want to change any configurations.

✓ Select Workload Platform

Edit

Workload Platform V-CENTER

> Create Workload Platform

Edit

✓ Manage Attributes

Edit

Included in Dictionary	Workload Attribute	Attribute Name in Dictionary	References
☒	vmid	vmid	--
☒	uuid	uuid	--
☒	os	os	--
☒	network	network	--
☒	macAddress	macAddress	--
☒	VM-Name	VM-Name	--

Exit Wizard

BackCreate

Overzichtspagina met het geselecteerde V-CENTER-werklastplatform en de kenmerken die in het woordenboek zijn opgenomen

10. Klik op Maken. Cisco ISE bevestigt het resultaat met het bericht Connection successfully created.



Succesmelding die bevestigt dat de werklstverbinding is gemaakt

De nieuwe vCenter-connector wordt weergegeven op de pagina Werklastverbindingen. De status is Verbinden terwijl Cisco ISE de sessie met vCenter instelt.

Workload Connections

Create [workload classification rules](#) to assign SGTs to IP addresses and receive mappings. Manage [Inbound SGT domain rules](#) to define the SXP domains that must receive the mappings. Manage [Outbound SGT domain rules](#) to define the data shared from Cisco ISE to Cisco ACI.

Q Search table						
0 Selected	+ Add Connection	More Actions ▾				
☐	Workload Connection Name ↕	Platform	Status	Received SGT Bindings	Sync Interval	Last Updated Time
☐	LAB_VCenter	VCENTER	Connecting	0	15 Minutes	--
1 Record(s)						

Pagina Verbindingen werklust met de nieuwe vCenter-connector in de status Verbinden

Stap 2. vCenter-kenmerken aan het woordenboek toevoegen (optioneel)

Voltooi deze stap alleen als u een aangepast kenmerk wilt toevoegen. De attributen die u kiest tijdens de stap Attributen beheren worden automatisch toegevoegd aan het vCenter-woordenboek, zodat de integratie hier zonder enige actie functioneert. Woordenboekattributen kunnen ook op elk moment worden beheerd nadat de verbinding is gemaakt:

1. Kies Werkcentra > TrustSec > Integraties > Werklustconnectors.
2. Klik op Eigenschappen woordenboek.
3. Klik op Attribuut toevoegen.
4. Schakel de schakeloptie Opnemen in woordenboek in.
5. Voer in het veld Attribuut Werklust de naam van het attribuut in, zoals het besturingssysteem.
6. Voer in het veld Attribuutnaam in het woordenboek de naam in die moet worden weergegeven.
7. Klik op Save (Opslaan).

Let op dit woordenboekgedrag:

- Per verbindingstype wordt één woordenboek gemaakt. Alle vCenter-connectors delen één vCenter-woordenboek.
- Attributen worden niet automatisch verwijderd wanneer een verbinding wordt verwijderd. Alle attributen die niet in gebruik zijn, kunnen handmatig worden verwijderd.
- Attributen kunnen worden geïmporteerd van de provider en attributen die niet aanwezig zijn in

de provider kunnen handmatig worden toegevoegd.

Stap 3. Werkbelastingen classificeren in SGT's

De werklasterclassificatieregels evalueren werklasterkenmerken, inclusief de geïmporteerde vCenter-tags, en wijzen SGT's toe. Deze stap levert de segmentatiewaarde van de integratie.

SGT-toewijzing gedraagt zich zoals beschreven in deze items:

- De primaire SGT is gemarkeerd als Security Group in het pxGrid-sessieonderwerp en wordt gebruikt om IP-naar-SGT-mappings te publiceren via SXP.
- Secundaire SGT's worden opgenomen in het onderwerp van de pxGrid-sessie als een geordende array met de naam Secundaire beveiligingsgroepen.
- Als meerdere regels overeenkomen en meerdere primaire SGT's toewijzen, wordt alleen de eerste toegewezen SGT als primair behandeld. De resterende SGT's worden secundair.

U maakt als volgt een classificatieregel voor dit voorbeeld:

1. Kies Werkcentra > TrustSec > Integraties > Werklasterclassificatie.
2. Klik op Classificatieregel toevoegen.
3. Voer in het gebied REGELINSTELLINGEN een regelnaam in en stel Status in op Enabled.
4. In het gebied AUTORISATIECONFIGURATIE kiest u in de vervolgkeuzelijst Primaire SGT de SGT die de regel toewijst, zoals [SGT_NAME]. In dit voorbeeld wordt de Production_Servers SGT toegewezen.
5. Kies optioneel in de vervolgkeuzelijst Secundaire SGT's (Optioneel) een of meer secundaire SGT's.
6. Bouw in het gebied REGELCONFIGURATIE de overeenkomende voorwaarde. Kies in de vervolgkeuzelijst met kenmerken een geïmporteerd vCenter-kenmerk, zoals Vcenter - os, kies de Equal-operator en voer de waarde in die moet worden aangepast. Dit voorbeeld komt overeen met CentOS 4/5 (64-bits).
7. Om de regel verder te verfijnen, klikt u op Toestand toevoegen en combineert u de voorwaarden met AND of OR. In dit voorbeeld wordt een IP-adres-voorwaarde toegevoegd die de IP Equals-operator gebruikt om de regel te beperken tot het enkele hostadres 192.168.10.33/32.
8. Klik optioneel op Voorbeeld om de SGT-details en de werklasterlastingen te bekijken die overeenkomen met de regel.
9. Klik op Add (Toevoegen).



Let op: de operator Equals vereist de volledige attribuutwaarde. vCenter rapporteert het gastbesturingssysteem als een volledige beschrijvende tekenreeks, zoals CentOS 4/5 (64-bits), niet als een korte naam zoals CentOS. Een regel die EqualOS toetst aan die waarde komt nooit overeen en faalt in stilte: de connector blijft werklasten importeren, maar er wordt geen SGT toegewezen. Bevestig de exacte waarde in Context Visibility voordat u de regel bouwt, zoals beschreven in het gedeelte Verify, of gebruik een operator zoals Bevat als u een reeks gastbesturingssystemen wilt matchen.

Add Classification Rule

RULE SETTINGS

Rule Name *

VM

Status

☒ Enabled ☐ Disabled

AUTHORIZATION CONFIGURATION

Primary SGT *

Production_Servers

Secondary SGTs (Optional)

RULE CONFIGURATION ⓘ

AND ▾	Vcenter - os ▾	Equals ▾	Label CentOS 4/5 (64-bit) Enter text to search	
	IP Address ▾	IP Equals ▾	Value * 192.168.10.33/32	
+ Add AND/OR Statement + Add Condition				

Voeg een pagina met classificatieregels toe waarin de primaire SGT van Production_Servers wordt toegewezen wanneer het kenmerk vCenter-besturingssysteem gelijk is aan CentOS 4/5 (64-bits) en het IP-adres gelijk is aan 192.168.10.33/32

Herhaal deze stappen voor elke extra groep werklasten die u wilt classificeren en wijs aan elke regel een andere primaire SGT toe.

Let op dit regelgedrag:

- Regels kunnen opnieuw worden geordend door slepen en neerzetten. Orde bepaalt de prioriteit.
- Een nieuwe regel of een dubbele regel kan worden ingevoegd voor of na een bestaande regel.
- De standaardclassificatieregel staat altijd onderaan de lijst, is standaard uitgeschakeld en

wordt toegewezen aan de Onbekende primaire SGT.

- Gebruik de optie Voorbeeld om SGT-details en overeenkomende regels te bekijken voordat u deze opslaat.

Stap 4. Routebindingen met inkomende en uitgaande SGT-domeinregels

SGT-domeinen bepalen welke delen van het netwerk specifieke SGT-bindingen ontvangen. Als er geen inkomende regels zijn gedefinieerd, worden bindingen die worden ontvangen van werklastconnectors naar het standaard SGT-domein verzonden.

Voeg een inkomende SGT-domeinregel toe:

1. Kies Werkcentra > TrustSec > SXP > Inbound & Outbound SGT-domeinregels.
2. Klik op het tabblad Inkomende SGT-domeinregels op Inkomende regel toevoegen.
3. Voer in het gebied Regelinstellingen een regelnaam in.
4. Klik op Ingeschakeld.
5. Kies in de vervolgkeuzelijst Bestemming de SGT-domeinen die de bindingen moeten ontvangen. Als u een domein wilt toevoegen, gebruikt u SGT-domein maken.
6. Bouw in het gebied Regelconfiguratie de voorwaarde op basis van kenmerken zoals SGT-naam, bron, IP-adres of een vCenter-kenmerk dat aan het woordenboek is toegevoegd, zoals het besturingssysteem. Combineer omstandigheden met AND en OR indien nodig.
7. Klik op Toevoegen en klik vervolgens op Opslaan.

Voeg een uitgaande SGT-domeinregel toe:

1. Open op dezelfde pagina het tabblad Uitgaande SGT-domeinregels en klik op Uitgaande regel toevoegen.
2. Voer een regelnaam in en klik op Ingeschakeld.
3. Kies in de vervolgkeuzelijst Bestemming de bestemmingen waarnaar de SGT's moeten worden verzonden.
4. Bouw in het gebied Regelconfiguratie de voorwaarde op basis van SGT-domeinen, SGT-naam of IP-adres.
5. Wijs in het gebied Contractconfiguratie Optioneel Verbruikte en geleverde contracten toe aan de gedeelde beveiligingsgroepen.
6. Klik op Toevoegen en klik vervolgens op Opslaan.

Gebruik de optie Voorbeeld om de overeenkomende IP-SGT-bindingen te bekijken terwijl u inkomende en uitgaande regels toevoegt of bewerkt.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De verbindingstatus controleren

Kies Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections en bevestig dat de vCenter-verbinding een Connected-status heeft. Vanaf deze pagina kunt u ook opnieuw verbinding maken, een verbinding opschorten of verwijderen.

Workload Connections

Create [workload classification rules](#) to assign SGTs to IP addresses and receive mappings. Manage [Inbound SGT domain rules](#) to define the SXP domains that must receive the mappings. Manage [Outbound SGT domain rules](#) to define the data shared from Cisco ISE to Cisco ACI.

Q Search table

0 Selected

[+ Add Connection](#)

[More Actions](#) ▾

☐	Workload Connection Name ↕	Platform	Status	Received SGT Bindings	Sync Interval	Last Updated Time
☐	LAB_VCenter	VCENTER	✔ Connected	0	15 Minutes	Jul 24, 2025, 3:10 PM

1 Record(s)

Pagina Verbindingen voor werklast met de vCenter-connector met de status Verbonden, het aantal ontvangen SGT-bindingen, het synchronisatieinterval en de laatst bijgewerkte tijd

De kolom Ontvangen SGT-bindingen leest 0 in deze afbeelding omdat de opname is gemaakt voordat een classificatieregel overeenkwam met een werklast. Een Connected status samen met een nulbindingtelling betekent dat Cisco ISE vCenter met succes heeft bereikt, maar nog geen SGT aan iets heeft toegewezen. Nadat een regel overeenkomt, rapporteert deze kolom het aantal bindingen dat Cisco ISE heeft afgeleid.

De beveiligingsgroepen controleren

Kies Werkcentra > TrustSec > Componenten > Beveiligingsgroepen en bevestig dat de verwachte SGT's bestaan. Bevestig in dit voorbeeld dat Production_Servers SGT bestaat.

Controleer de IP-SGT-bindingen

Kies Werkcentra > TrustSec > SXP > SGT-bindingen en bevestig dat de IP-adressen van de werklust gebonden zijn aan de juiste SGT's, met de juiste bron en toegepaste classificatieregel.

De werkbelasting tijdens live sessies controleren

Kies Bewerkingen > Werklusten > Live sessie, waarmee de pagina Werklust Live sessies wordt geopend. Live sessies kunnen alleen worden bekeken op de primaire Policy Administration Node (PAN). Op deze pagina kunnen sessies worden gefilterd op connectortype, kolommen worden getoond, verborgen en opnieuw worden gerangschikt, resultaten kunnen worden gesorteerd, filters kunnen worden opgeslagen en gegevens kunnen worden geëxporteerd in CSV- of PDF-indeling.

Workload Live Sessions

 [Open To](#)

Initiated	SGT Bindings	SGT Name	Secondary SGTs	Source	Destinations	Inbound SGT Domain Rules	SGT Domains
X	SGT Bindings	SGT Name	Secondary SGTs	Source	Destinations	Inbound SGT Domain Rules	SGT Domains
Aug 02, 2026 06:02 AM	192.168.10.73	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.120	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.5	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.75	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.2	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.102	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.226	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.241	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.72	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.101	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.254	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.243	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.242	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.1	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.74	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.11	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.33	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.80	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.76	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.245	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.68	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.227	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2026 06:02 AM	192.168.10.13	---	---	LAB_VCenter	---	Default Filter	default

De tabel met werkbelasting live sessies bevat één rij per aangeleerde werkbelasting, met de geïnitieerde tijdstempel, het IP-adres van de SGT-bindingen, de lege SGT-naam, secundaire SGT's en bestemmingskolommen, de bronverbindingsnaam LAB_VCenter en de inkomende SGT-domeinregels en SGT-domeinkoppelingen met de tekst Standaardfilter en standaard



Opmerking: deze opname wordt bijgesneden in de kolommen die gegevens bevatten in dit voorbeeld. De kolommen Outbound SGT Domain Rules en Workload Classification Rules

gaan verder naar rechts van het zichtbare gebied en zijn leeg op elke rij, net als de ACI-specifieke kolommen daarachter. Deze pagina is vastgelegd in een latere laboratoriumsessie dan de verbindingsconfiguratiepagina's, dus de geïnitieerde tijdstempels komen niet overeen met de laatst bijgewerkte tijd die eerder op de pagina Werklastverbindingen is weergegeven.

Elke rij vertegenwoordigt één werklast die Cisco ISE heeft geleerd van een connector. Gebruik deze kolommen om de integratie te bevestigen:

zuil	Wat het bevestigt
ingewijd	Het tijdstip waarop Cisco ISE de sessie heeft geleerd. Recente tijdstempels bevestigen dat de connector aan het pollen is.
SGT-bindingen	Het IP-adres van de werklast dat Cisco ISE van vCenter heeft ontvangen.
bron	De werklastverbinding die de sessie heeft gemeld. Bevestigt van welke connector de gegevens afkomstig zijn.
Inkomende SGT-domeinregels en SGT-domeinen	De domeinregel en het SGT-domein die op de sessie zijn toegepast. Selecteer een link om de overeenkomende regel te bekijken.
SGT-naam, secundaire SGT's en werklastclassificatieregels	De SGT's die aan de werklast zijn toegewezen en de regel die ze heeft toegewezen. Deze kolommen blijven leeg voor werklasten waarvoor geen classificatieregel overeenkomt.

Gebruik de besturingselementen Vernieuwen, Weergeven en Binnen in de rechterbovenhoek van de pagina, rechts van het bijgesneden gebied, om het vernieuwingsinterval, het aantal records en het tijdvenster in te stellen.

In deze afbeelding is de kolom SGT-bindingen volledig ingevuld, terwijl de SGT-naam en secundaire SGT's op elke rij leeg zijn, omdat de opname is gemaakt voordat een classificatieregel is afgestemd. De kolom Werklastclassificatieregels, die buiten het bijgesneden gebied ligt, is om dezelfde reden leeg. Deze combinatie is op zichzelf al een nuttige diagnose: het bevestigt dat de connector op de juiste manier werklasten uit vCenter ophaalt en dat het probleem eerder in de regelcondities ligt dan in de verbinding. Wanneer u het ziet, keert u terug naar stap 3 en controleert u de overeenkomende waarden met de attribuutwaarden die Context Visibility

rapporteert, zoals beschreven in de waarschuwing in die stap.

Zichtbaarheid van werkbelasting in context controleren

 Versievereiste: het dashboard Workload Connector Endpoints is beschikbaar vanaf Cisco ISE 3.5 Patch 3. Gebruik in Cisco ISE 3.4 de pagina Workload Live Sessions zoals beschreven in de vorige sectie.

Cisco ISE biedt een speciaal Workload Connector Endpoints dashboard binnen Context Visibility. Het verzamelt, analyseert en rapporteert de eindpuntattribuutgegevens die zijn verzameld via werklasterconnectors in één filterbare weergave.

Zo opent u de weergave:

1. Kies in de Cisco ISE GUI Context Visibility > Endpoints.
2. Open het tabblad Werklasterconnector-eindpunten. Als het tabblad niet zichtbaar is in de tabstrip, klikt u op Meer.
3. Kies in de vervolgkeuzelijst Connector de werklasterverbinding waarvan u de eindpunten wilt controleren.

In het venster worden de gegevens van het eindpuntkenmerk weergegeven die worden opgehaald uit de werklasterconnectors. Elke rij identificeert een eindpunt op IP-adres, sourceType en Connectornaam.

Workload Connector Endpoints Rows/Page 25 1 / 1 > > Go 23 Total Rows

This window lists the endpoint attribute data that is fetched from Workload Connectors. Click Connector - LAB_VCenter or download the endpoint details. To create a Workload Connector or to update existing connector configurations, go to the Workload Connectors window.

Export Filter

IP Address	visibility.column.label.source...	Connector Name
IP Address	visibility.column.label.sourceType	Connector Name
192.168.10.1	Vcenter	LAB_VCenter
192.168.10.120	Vcenter	LAB_VCenter
192.168.10.226	Vcenter	LAB_VCenter
192.168.10.227	Vcenter	LAB_VCenter
192.168.10.241	Vcenter	LAB_VCenter
192.168.10.33	Vcenter	LAB_VCenter
192.168.10.68	Vcenter	LAB_VCenter
192.168.10.72	Vcenter	LAB_VCenter
192.168.10.73	Vcenter	LAB_VCenter

Werkbelasting Connector-eindpunten onder Contextzichtbaarheid, met vermelding van vCenter-eindpunten voor werkbelasting op IP-adres, brontype en connectornaam, waarbij de vervolgkeuzelijst Connector is ingesteld op LAB_VCenter, de optie Exporteren,

Vanuit deze visie kunt u:

- Filter de lijst. Gebruik de filterrij onder de kolomkoppen om de resultaten te verfijnen op IP-adres, brontype of connectornaam. Filters zijn additief, dus elke waarde die u toepast verfijnt de resultaatset verder.
- Pagina door de resultaten. Gebruik het besturingselement Rijen/Pagina en de paginatiepijlen om de paginagrootte te wijzigen en tussen pagina's te verplaatsen. Het totale aantal eindpunten verschijnt rechts van de pijlen, hier weergegeven als 23 Totale rijen.
- Exporteer de gegevens. Klik op Exporteren om de vermelde eindpuntgegevens te downloaden.
- Inspecteer een eindpunt. Klik op het IP-adres van een eindpunt om het deelvenster Details te openen.

In het deelvenster Details wordt elk kenmerk weergegeven dat Cisco ISE voor het geselecteerde eindpunt heeft. Klik op Downloaden om de attribootgegevens op te slaan of klik op Annuleren om het deelvenster te sluiten.

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

Het deelvenster Details voor een geselecteerd eindpunt voor de werklust, met de titel Details boven de naam en het eindpunt van de connector, met de lijst ATTRIBUTEN van vCenter-eigenschappen die Cisco ISE voor die virtuele machine heeft verzameld en de besturingselementen Annuleren en downloaden

Het deelvenster wordt geïdentificeerd door de naam van de werklustverbinding en het adres van het eindpunt, hier weergegeven als LAB_VCenter_192.168.10.1. Voor een vCenter-eindpunt voor de werklust omvatten de kenmerken de eigenschappen van de virtuele machine die zijn geleerd van vCenter, zoals Power, VM-Name, host, macAddress, network, os, uuid, vmid en vmtype, samen met de connector-metagegevenscorrelatielid, source, ipAddress, connectorType en SourceType. Elke aangepaste vCenter-tag die u aan het woordenboek hebt toegevoegd, wordt ook hier weergegeven.

Dit venster is de gezaghebbende bron voor de waarden die uw classificatieregels moeten overeenkomen, en als u dit eerst controleert, voorkomt u de meest voorkomende fout in deze workflow. In deze afbeelding leest os CentOS 4/5 (64-bits), wat de volledige tekenreeks is die een Equal-voorwaarde moet reproduceren. Lees hier de waarde voordat u de regel in stap 3 schrijft, in plaats van een korte vorm zoals CentOS aan te nemen.



Opmerking: voor elk eindpunt worden maximaal 50 kenmerken weergegeven.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Veelvoorkomende problemen

Symptoom	Vermoedelijke oorzaak	Actie
Testverbinding is mislukt tijdens het instellen van de connector	Een of meer verbindingsgegevens zijn onjuist of aan een vereiste is niet voldaan	Controleer het FQDN- of IP-adres en controleer of het overeenkomt met het SAN-certificaat. Controleer de gebruikersnaam en het wachtwoord, bekijk de

Symptoom	Vermoedelijke oorzaak	Actie
		certificaatvalidatie-instelling en bevestig dat aan de vereisten voor proxybypass en tijdsynchronisatie is voldaan.
Connector wordt gemaakt, maar er worden geen gegevens geïmporteerd	Cisco ISE kan public.ecr.aws niet bereiken	Bevestig dat de proxy of firewall HTTPS-verkeer op TCP-poort 443 naar deze URL toestaat.
Werkbelastingen worden geïmporteerd, maar er wordt geen SGT toegewezen en ontvangen SGT-bindingen blijven op 0.	Een voorwaarde voor een classificatieregel komt niet overeen met de werkelijke waarde van het kenmerk. Een Equal-voorwaarde die is getest tegen een partiële waarde, zoals CentOS in plaats van CentOS 4/5 (64-bits), is de meest voorkomende oorzaak	Open het deelvenster Details in Context Visibility, lees de exacte attribuutwaarde en corrigeer de regelvoorwaarde of wijzig de operator in Bevat. Deze storing is stil: er wordt geen alarm geplaatst, omdat de connector zelf gezond is.
Verbinding verplaatst naar Opgeschorte status	Alle SGT's die aan de verbinding zijn gekoppeld, zijn verwijderd	Maak de vereiste SGT's opnieuw aan en herstel de verbinding. De bijbehorende SXP-bindingen en MnT-sessiegegevens worden verwijderd terwijl de verbinding wordt opgeschort.
Verbindingsgegevens ontbreken na herstart PSN	Sessiegegevens zijn niet opnieuw gevuld	Schakel de verbinding uit en maak deze vervolgens opnieuw verbinding.

Foutopsporingslogboeken inschakelen

Stel de ernst van het foutopsporingslogboek voor de component Workload Connector in op DEBUG op de PAN-, SXP- en pxGrid-nodes vanuit Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration.

Deze logbestanden zijn beschikbaar in /opt/CSCOcpm/logs:

Logbestand	tevreden
werklasten.log	Werkbelasting connector bewerkingen.
Werklast-conn/*.log	Logboeken per verbinding.
API-service.log	API-serviceactiviteit.
ise-psc.log	Cisco ISE-beleidsserviceactiviteit.
pxgriddirect-service.log	pxGrid Direct-serviceactiviteit.
sxp_appserver/sxp.log	SXP-bindende distributie.

alarm

Cisco ISE genereert deze alarmen voor vCenter en andere cloudconnectors:

alarm	Gestegen wanneer
Werklastverbinding maken/verbinden mislukt	Het maken van een connector mislukt na een gebeurtenis zoals een terugzetprocedure, een promotie- of HA-gebeurtenis of een upgrade.
Werklastverbinding Verwijderen mislukt	Het verwijderen van de connector mislukt.
Fout bij werklastverbinding	Een andere gerelateerde servicefout treedt op.

Gerelateerde informatie

- [Cisco ISE Common Policy and Workload Connectors](#)
- [Cisco ISE vereiste internet-URL's](#)
- [Cisco ISE 3.5-beheerdershandleiding](#)
- [Cisco technische ondersteuning en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.