

VMware vCenter와 ISE 워크로드 커넥터 통합 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[Cisco ISE](#)

[VMware vCenter](#)

[연결](#)

[인증서](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[주요 조건](#)

[사용된 자리 표시자](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[1단계. vCenter 워크로드 연결 추가](#)

[2단계. 사전에 vCenter 특성 추가\(선택 사항\)](#)

[3단계. 워크로드를 SGT로 분류](#)

[4단계. 인바운드 및 아웃바운드 SGT 도메인 규칙과의 바인딩 경로](#)

[다음을 확인합니다.](#)

[연결 상태 확인](#)

[보안 그룹 확인](#)

[IP-SGT 바인딩 확인](#)

[워크로드 라이브 세션 확인](#)

[Context Visibility에서 워크로드 가시성 확인](#)

[문제 해결](#)

[일반적인 문제](#)

[디버그 로그 사용](#)

[알람](#)

[관련 정보](#)

소개

이 문서에서는 VMware vCenter용 Cisco ISE 워크로드 커넥터를 구성하여 워크로드 컨텍스트를 가져오고 그룹 기반 세그멘테이션을 적용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 관리
- VMware vCenter 관리
- SGT(Security Group Tag), SXP(SGT Exchange Protocol) 및 pxGrid를 비롯한 Cisco TrustSec 개념

vCenter 워크로드 연결을 추가하기 전에 이러한 조건이 충족되는지 확인합니다.

Cisco ISE

- pxGrid는 구축에서 하나 이상의 노드에서 활성화되어 있습니다.
- SXP는 구축에서 하나 이상의 노드에서 활성화되어 있습니다.

VMware vCenter

- 읽기 전용 권한이 있는 vCenter 계정을 사용할 수 있습니다. 커넥터는 읽기 작업만 수행합니다.
- 가져올 vCenter 특성 또는 태그가 식별되었습니다. 이 문서에서는 os 특성을 예로 사용합니다.

연결

- Cisco ISE는 Workload Connector 기능에 필요한 public.ecr.aws에 연결할 수 있으므로 Cisco ISE에서 안정적인 인터넷 연결을 사용할 수 있습니다. 프록시 서버 또는 방화벽이 경로에 있는 경우 Cisco ISE와 이 URL 간의 HTTPS(TCP 포트 443) 트래픽을 허용합니다. 이 URL에 연결할 수 없는 경우 워크로드 커넥터가 의도한 대로 작동하지 않습니다.
- 프록시가 인터넷 액세스에 사용되고 vCenter가 온프레미스에 구축된 경우 vCenter IP 주소에 대한 프록시 우회를 구성합니다.

인증서

- 인증서 검증을 사용하는 경우 vCenter에 대해 입력한 FQDN 또는 IP 주소가 vCenter 엔드포인트 인증서의 SAN(주체 대체 이름)과 일치해야 합니다.

- vCenter 루트 인증서는 Cisco ISE Trusted Certificates 저장소로 가져올 수 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine), 릴리스 3.4, 커넥터 구성 및 확인 절차에 사용
- Cisco ISE(Identity Services Engine), 릴리스 3.5 패치 3, 상황 가시성 절차에만 사용
- VMware vCenter Server 8.0 업데이트 3



참고: Context Visibility의 Workload Connector Endpoints 대시보드에는 Cisco ISE 3.5 Patch 3 이상이 필요하므로 해당 섹션에 있는 두 이미지가 해당 릴리스에서 캡처되었습니다. 이 문서의 다른 모든 절차 및 이미지는 Cisco ISE 3.4에서 제공됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

오늘날의 데이터 센터는 역동적입니다. VM(가상 머신)은 지속적으로 생성, 이동 및 폐기되며 IP 주소는 VM과 함께 변경됩니다. 고정 IP 주소 또는 서브넷에 의존하는 보안 정책은 이러한 변화의 속도를 따라갈 수 없으므로 시행과 가시성 모두에서 격차가 발생합니다.

Cisco ISE는 공통 정책 프레임워크 및 해당 워크로드 커넥터를 통해 이 문제를 해결합니다. 워크로드 커넥터는 데이터 센터 또는 클라우드 플랫폼에 대한 보안 연결을 설정하고, 여기에서 실행되는 애플리케이션 워크로드의 컨텍스트를 가져온 다음, 해당 컨텍스트를 SGT로 표준화하고, 그 결과를 네트워크의 나머지 영역과 공유하여 정책을 작성할 수 있도록 합니다.

vCenter는 게스트 운영 체제, 연결된 포트 그룹 및 전원 상태와 같은 특성 집합을 통해 모든 가상 머신에 대해 이미 설명합니다. VMware 관리자는 환경, 애플리케이션 계층, 소유자 또는 사업부와 같은 메타데이터를 전달하는 사용자 지정 태그를 사용하여 설명을 확장합니다. vCenter Workload Connector는 둘 다 가져오고 이를 SGT로 변환합니다. 이를 통해 다음과 같은 세 가지 결과를 얻을 수 있습니다.

- 정책은 워크로드를 기반으로 합니다. VM을 이동하거나 주소를 다시 지정하면 특성 기반 SGT가 그대로 유지되므로 수동 업데이트 없이 세그멘테이션이 계속 작동합니다.

- 기존 컨텍스트가 재사용됩니다. Cisco ISE는 vCenter에서 이미 유지 관리 하는 속성 및 태그를 사용 하므로 새로운 분류 체계는 필요 하지 않습니다.
- 세그멘테이션은 일관적입니다. SGT는 TrustSec 지원 네트워크에서 배포되므로 모든 시행 지점에서 동일한 정책이 적용됩니다.

이 문서에서는 실행 중인 단일 예제를 사용합니다. vCenter에서 각 가상 머신에 대해 보고하는 os 특성(이 Lab에서 CentOS 4/5(64비트)을 읽고 Cisco ISE로 가져오고 IP 주소 조건과 결합하므로 일치하는 워크로드가 Production_Servers 보안 그룹에 자동으로 배치됩니다. 그런 다음 이러한 워크로드는 수동으로 추적한 IP 주소가 아닌 그룹 멤버십을 기준으로 세분화됩니다. vCenter에서 표시하는 다른 특성 또는 사용자 지정 태그에도 동일한 절차가 적용됩니다.

주요 조건



참고: VMware ESXi는 태그를 지원하지 않습니다. 따라서 vCenter만 워크로드 커넥터로 구성할 수 있습니다. 독립형 ESXi 호스트는 사용할 수 없습니다.

용어	정의
트러스트섹 (TrustSec)	그룹 기반 세그멘테이션을 위한 Cisco 기술이며, IP 주소 대신 그룹을 대상으로 정책이 작성됩니다.
SGT(보안 그룹 태그)	프로덕션 워크로드와 같이 그룹을 나타내며 정책 시행의 기반으로 사용되는 태그입니다.
SXP(SGT Exchange Protocol)	IP-SGT 바인딩을 시행 디바이스에 배포하는 데 사용되는 프로토콜입니다.
pxGrid	Cisco ISE와 다른 시스템 간에 세션 및 SGT와 같은 컨텍스트를 공유하는 데 사용되는 Cisco 플랫폼입니다.
공통 정책	데이터 센터 및 클라우드에 연결하고 컨텍스트를 SGT로 표준화한 다음 여러 도메인에 공유하는 Cisco ISE 프레임워크입니다.
워크로드 커넥터	vCenter, AWS, Azure, GCP 또는 ACI에 연결하고 워크로드 컨텍스트를 가져오는 Cisco ISE 구성 요소입니다.

사용된 자리 표시자

대괄호 안의 값은 자리 표시자입니다. 해당 환경에 적용되는 값으로 대체합니다.

자리 표시자	설명
[VCENTER_FQDN]	vCenter 서버의 정규화된 도메인 이름입니다.
[VCENTER_IP_ADDRESS]	vCenter 서버의 IP 주소입니다.
[사용자 이름]	vCenter 읽기 전용 계정 사용자 이름입니다.
[암호]	vCenter 읽기 전용 계정 비밀번호입니다.
[SGT_NAME]	분류 규칙에 의해 할당된 보안 그룹 태그의 이름입니다.
[VM_NAME]	vCenter에 있는 가상 머신의 이름입니다.
[VM_UUID]	vCenter에 있는 가상 머신의 UUID입니다.
[VM_ID]	가상 머신의 vCenter 관리 개체 참조
[호스트 ID]	ESXi 호스트의 vCenter 관리 객체 참조.
[네트워크 이름]	vCenter 포트 그룹 또는 네트워크의 이름입니다.

이 문서의 이미지는 작업 로드 연결 이름 LAB_VCenter, vCenter 주소 192.168.1.50 및 작업 로드 서브넷 192.168.10.0/24을 사용하는 실습에서 가져온 것입니다. 환경에 적용되는 이름 지정 및 주소 지정으로 대체합니다.

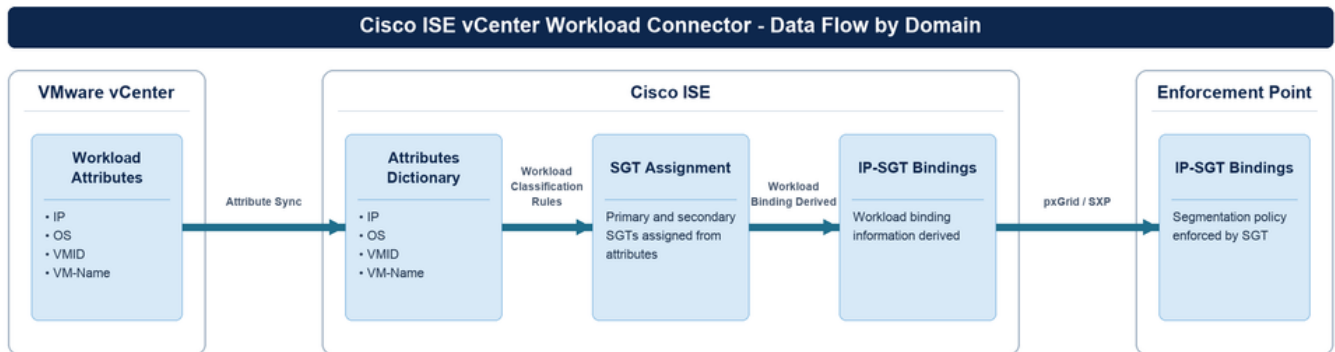
구성

네트워크 다이어그램

이 통합은 vCenter 메타데이터를 5단계로 시행 가능한 정책으로 변환합니다.

1. Cisco ISE vCenter Workload Connector는 vCenter에서 워크로드 특성 및 태그를 읽습니다.

2. 선택한 특성은 Cisco ISE 특성 사전에 추가되어 규칙에서 참조될 수 있습니다.
3. 워크로드 분류 규칙은 이러한 특성을 평가하고 각 워크로드에 기본 SGT 및 선택적으로 하나 이상의 보조 SGT를 할당합니다.
4. Cisco ISE는 IP-SGT 바인딩을 파생하고 SXP 및 pxGrid를 통해 게시합니다. 인바운드 및 아웃바운드 SGT 도메인 규칙은 어떤 SGT 도메인이 바인딩을 수신하는지, 그리고 이들이 공유되는 위치를 제어합니다.
5. 시행 포인트는 SGT를 적용하여 트래픽을 허용하거나 거부합니다.



Cisco ISE vCenter Workload Connector 데이터 흐름은 세 가지 도메인 전반에 걸쳐 이루어집니다. vCenter는 워크로드 특성(IP, OS, VMID, VM-Name)을 제공합니다. Cisco ISE는 속성 사전에 저장 하고, 1 주 루트 브리지 와 보조 SGT를 할당 하기 위해 작업 로드 분류 규칙을 적용 하고, IP-SGT 바인딩을 도출 합니다. 바인딩은 pxGrid 및 SXP를 통해 시행 포인트로 공유됩니다

설정

1단계. vCenter 워크로드 연결 추가

1. Cisco ISE GUI에서 메뉴 아이콘을 클릭하고 Work Centers(작업 센터) > TrustSec > Integrations(통합) > Workload Connectors(워크로드 커넥터) > Workload Connections(워크로드 연결)를 선택합니다.
2. Add Connection(연결 추가)을 클릭합니다.

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.

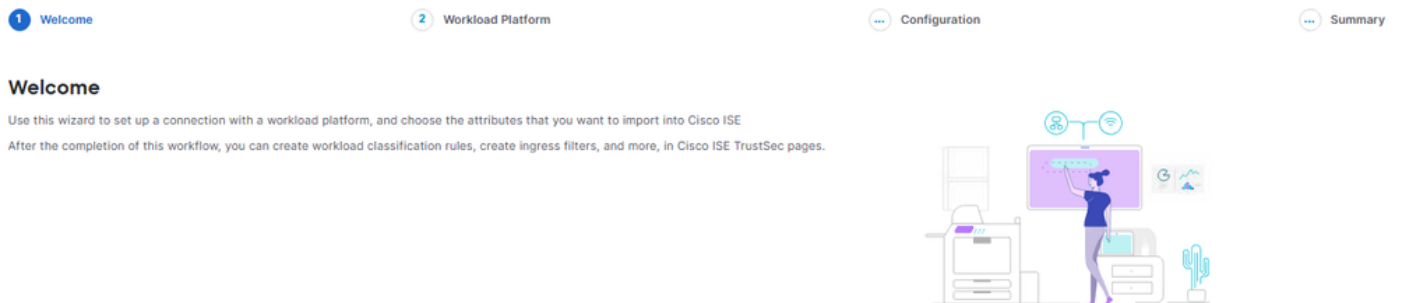


No Workload Connected

Add Connection

구성된 연결이 없는 [작업 로드 연결] 페이지에 [연결 추가] 단추 표시

3. Let's do it을 클릭합니다.



작업 로드 연결 마법사 시작 페이지 - 마법사의 시작, 작업 로드 플랫폼, 구성 및 요약 단계를 표시합니다.

4. Select Workload Platform(워크로드 플랫폼 선택) 페이지에서 vCenter를 선택하고 Next(다음)를 클릭합니다.

Welcome
Workload Platform
Configuration
Summary

Select Workload Platform

Choose a workload platform to configure the connection with.

ACI

Connect with Cisco ACI to share SGTs and IP-SGT bindings with a Cisco ACI fabric and/or receive Endpoint Group (EPG), Endpoint Security Group (ESG), and endpoint configuration information from a Cisco ACI fabric.

AWS

Create a connection with your AWS account to import your application workloads into Cisco ISE.

Azure

Create a connection with your Azure account to import your application workloads into Cisco ISE.

vCenter

Create a connection with your VMware vCenter account to import your application workloads into Cisco ISE.

GCP

Create a connection with your GCP account to import your application workloads into Cisco ISE.

ACI, AWS, Azure 및 GCP 플랫폼 중에서 vCenter 옵션이 선택된 워크로드 플랫폼 선택 페이지

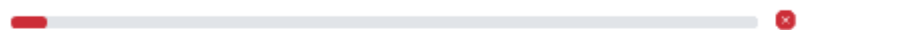
5. Create Workload Connection(워크로드 연결 생성) 페이지에서 Cisco ISE는 Workload Connector 서비스가 연결 세부사항을 승인하기 전에 실행 중인지 확인합니다.

서비스가 아직 실행되고 있지 않으면 Workload Connector Services가 실행되고 있지 않음을 페이지에 보고합니다.

Create Workload Connection

Checking Prerequisites

Workload Connector Services are not running



Non-editable after creation

Description

Sync Interval*

Minutes



Hint

☐ Validate vCenter certificate. ⓘ

그런 다음 Cisco ISE는 자동으로 서비스를 시작하고 진행 상황을 표시합니다.

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. [?](#)

Workload Connector 서비스 시작을 보여주는 [Workload Connection 생성] 페이지

페이지에서 Workload Connector Services가 실행 중임을 보고할 때까지 기다립니다. 연결 세부 정보 필드는 이 검사가 성공한 후에만 완료할 수 있습니다.

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. ⓘ

Workload Connector 서비스가 실행 중임을 확인하는 [Workload Connection 생성] 페이지

6. 연결 세부 정보를 입력합니다.

필드	설명
작업 로드 연결 이름	문자, 숫자 및 밑줄을 사용하는 고유한 이름입니다. 최대 32자이며 공백은 없습니다. 이 예에서는 LAB_VCenter를 사용합니다.
설명	연결에 대한 설명입니다.
동기화 간 격	Cisco ISE가 vCenter에서 데이터를 업데이트하는 빈도 유효한 범위는 60초~7일 입니다. 기본값은 15분입니다. 간격이 짧으면 데이터를 더 자주 새로 고침하지만 성능에 영향을 줄 수 있습니다.
FQDN 또 는 IP 주소	vCenter의 호스트 이름 또는 IP 주소(예: [VCENTER_FQDN] 또는 [VCENTER_IP_ADDRESS])입니다. 이 값은 vCenter 엔드포인트 인증서의 주체 대체 이름과 일치해야 합니다.

필드	설명
사용자	vCenter 어카운트 사용자 이름 [USERNAME].
암호	vCenter 계정 비밀번호 [PASSWORD].
vCenter 인증서 검증	선택 사항. 인증서를 검증하고 vCenter 루트 인증서를 Cisco ISE Trusted Certificates 저장소로 가져옵니다. 가져오는 동안 Trust for authentication of Cisco Services(Cisco 서비스 인증에 대한 신뢰)도 선택합니다. 프로덕션 환경에는 인증서 검증이 권장됩니다.

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. ⓘ

완료된 vCenter 연결 세부 정보 필드 및 vCenter 인증서 검증 확인란이 선택된 작업 로드 연결 생성 페이지

이 그림에서 사용자 필드는 자리 표시자를 표시합니다. 환경에 적용되는 자격 증명을 입력합니다.



참고: Cisco ISE는 사용자가 입력 한 정보를 확인 합니다. 세부 정보가 올바르지 않으면 Cisco ISE는 Test connection failed(연결 테스트 실패) 오류를 반환합니다.

7. Next(다음)를 클릭합니다. Cisco ISE는 연결을 테스트하고 Test connection successful(연결

테스트 성공) 메시지를 통해 결과를 확인합니다.



vCenter에 대한 테스트 연결이 성공했음을 확인하는 성공 알림

vCenter에 대한 테스트 연결이 성공했음을 확인하는 성공 알림

8. Manage Attributes(특성 관리) 페이지에서 Cisco ISE 사전에 추가할 vCenter 특성을 선택합니다. 이 예에서는 os 특성이 포함되어 있는지 확인합니다. 그런 다음 Next(다음)를 클릭합니다.

- 모든 학습된 특성을 한 번에 포함하려면 사전에 모두 포함 토글을 활성화합니다.
- 속성의 이름을 바꾸려면 사전의 속성 이름 필드를 편집합니다.
- 계속하려면 적어도 하나의 특성을 추가해야 합니다.
- ^, =, ", \, 등의 특수 문자가 포함된 속성 이름 |, :, [또는] 은(는) 유효하지 않으므로 추가할 수 없습니다.

☒ 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	--

Include All in Dictionary(사전에 모두 포함) 토글이 활성화되고 학습된 vCenter 특성이 나열된 속성 관리 페이지

목록을 스크롤하여 vmid, uuid, os, network, macAddress, VM-Name, host, Power, guest.FullName 등 vCenter에서 연결을 학습한 모든 특성을 검토합니다.

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: 10 1 - 9 < 1 >			

Manage Attributes(특성 관리) 페이지를 스크롤하여 학습된 vCenter 특성의 전체 목록 및 레코드 수를 표시합니다.

9. Summary(요약) 페이지에서 컨피그레이션을 검토합니다. 해당 값을 변경하려면 섹션 옆의 Edit를 클릭합니다.

Welcome
Workload Platform
Create Workload Connection
Manage Attributes
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
Back Create

선택한 V-CENTER 워크로드 플랫폼 및 사전에 포함된 속성을 보여 주는 요약 페이지

10. Create(생성)를 클릭합니다. Cisco ISE는 Connection successfully created(연결이 성공적으로 생성됨) 메시지로 결과를 확인합니다.



작업 로드 연결이 생성되었음을 확인하는 성공 알림

새 vCenter 커넥터가 Workload Connections(작업 로드 연결) 페이지에 나타납니다. Cisco ISE가 vCenter를 사용하여 세션을 설정하는 동안 상태가 Connecting(연결)입니다.

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)						

연결 중 상태의 새 vCenter 커넥터를 나열하는 작업 로드 연결 페이지

2단계. 사전에 vCenter 특성 추가(선택 사항)

사용자 지정 특성을 추가하려는 경우에만 이 단계를 완료합니다. 속성 관리 단계 중에 선택한 속성은 vCenter 사전에 자동으로 추가되므로 통합은 별도의 작업 없이 작동합니다. 연결이 생성된 후 언제든지 사전 특성을 관리할 수 있습니다.

1. Work Centers(작업 센터) > TrustSec > Integrations(통합) > Workload Connectors(워크로드 커넥터)를 선택합니다.
2. Attributes Dictionary를 클릭합니다.
3. Add Attribute(특성 추가)를 클릭합니다.
4. Include in Dictionary(사전에 포함) 토글을 활성화합니다.
5. Workload Attribute 필드에 os와 같은 특성 이름을 입력합니다.
6. Attribute Name in Dictionary(사전의 특성 이름) 필드에 표시할 이름을 입력합니다.
7. 저장을 클릭합니다.

이 사전 동작에 유의하십시오.

- 연결 유형당 하나의 사전이 생성됩니다. 모든 vCenter 커넥터는 단일 vCenter 사전을 공유합니다.
- 연결이 삭제되어도 특성은 자동으로 제거되지 않습니다. 사용 중이 아닌 속성은 수동으로 삭제할 수 있습니다.
- 특성은 공급자에서 가져올 수 있으며, 공급자에 없는 특성은 수동으로 추가할 수 있습니다.

3단계. 워크로드를 SGT로 분류

워크로드 분류 규칙은 가져온 vCenter 태그를 포함하여 워크로드 속성을 평가하고 SGT를 할당합니다. 이 단계에서는 통합의 세그멘테이션 가치를 제공합니다.

SGT 할당은 다음 항목에 설명된 대로 작동합니다.

- 기본 SGT는 pxGrid 세션 항목에서 보안 그룹으로 표시되며 SXP를 통해 IP-SGT 매핑을 게시하는 데 사용됩니다.
- 보조 SGT는 Secondary Security Groups(보조 보안 그룹)라는 순서가 지정된 어레이로서 pxGrid 세션 항목에 포함됩니다.
- 여러 규칙이 일치하고 여러 기본 SGT를 할당하는 경우 처음 할당된 SGT만 기본 SGT로 처리됩니다. 나머지 SGT는 보조 SGT가 됩니다.

이 예에 대한 분류 규칙을 생성하려면

1. Work Centers(작업 센터) > TrustSec > Integrations(통합) > Workload Classification(워크로드 분류)을 선택합니다.
2. Add Classification Rule을 클릭합니다.
3. RULE SETTINGS(규칙 설정) 영역에서 Rule Name(규칙 이름)을 입력하고 Status(상태)를

Enabled(활성화됨)로 설정합니다.

4. AUTHORIZATION CONFIGURATION(권한 부여 컨피그레이션) 영역의 Primary SGT(기본 SGT) 드롭다운 목록에서 규칙이 할당하는 SGT(예: [SGT_NAME])를 선택합니다. 이 예에서는 Production_Servers SGT를 할당합니다.
5. 선택적으로, Secondary SGTs (Optional)(보조 SGT(선택 사항)) 드롭다운 목록에서 하나 이상의 보조 SGT를 선택합니다.
6. RULE CONFIGURATION 영역에서 일치 조건을 작성합니다. 특성 드롭다운 목록에서 가져온 vCenter 특성(예: Vcenter - os)을 선택하고 같음 연산자를 선택한 다음 일치시킬 값을 입력합니다. 이 예에서는 CentOS 4/5(64비트)와 일치합니다.
7. 규칙을 더 좁히려면 Add Condition을 클릭하고 AND 또는 OR로 조건을 결합합니다. 이 예에서는 IP Equals 연산자를 사용하여 규칙을 단일 호스트 주소 192.168.10.33/32으로 제한하는 IP 주소 조건을 추가합니다.
8. 선택적으로, Preview를 클릭하여 SGT 세부사항 및 규칙이 일치하는 워크로드를 검토합니다.
9. Add(추가)를 클릭합니다.



주의: Equals 연산자에는 전체 특성 값이 필요합니다. vCenter는 게스트 운영 체제를 CentOS와 같은 짧은 이름이 아닌 전체 설명 문자열(예: CentOS 4/5(64비트))로 보고합니다. 해당 값에 대해 Equals CentOS를 테스트하는 규칙은 일치하지 않으며 자동으로 실패합니다. 커넥터가 계속해서 워크로드를 가져오지만 SGT는 할당되지 않습니다. Verify 섹션에 설명된 대로 규칙을 작성하기 전에 Context Visibility에서 정확한 값을 확인하거나 게스트 운영 체제 패밀리를 매칭하려면 Contains와 같은 연산자를 사용합니다.

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

vCenter os 특성이 CentOS 4/5(64비트)와 IP 주소가 192.168.10.33/32인 경우 Production_Servers 기본 SGT를 할당하는 분류 규칙 추가 페이지

분류할 각 추가 워크로드 그룹에 대해 이러한 단계를 반복하고 각 규칙에 다른 기본 SGT를 할당합니다.

이 규칙 동작에 유의하십시오.

- 끌어서 놓기를 통해 규칙의 순서를 변경할 수 있습니다. 순서에 따라 우선 순위가 결정됩니다.
- 새 규칙 또는 중복 규칙은 기존 규칙의 앞이나 뒤에 삽입할 수 있습니다.
- 기본 분류 규칙은 항상 목록의 맨 아래에 있으며, 기본적으로 비활성화되어 있으며, Unknown 기본 SGT에 매핑됩니다.
- 저장하기 전에 Preview 옵션을 사용하여 SGT 세부사항 및 일치하는 규칙을 검토할 수 있습니다

4단계. 인바운드 및 아웃바운드 SGT 도메인 규칙과의 바인딩 경로

SGT 도메인은 네트워크의 어느 부분이 특정 SGT 바인딩을 수신할지를 제어합니다. 인바운드 규칙이 정의되지 않은 경우 워크로드 커넥터에서 받은 바인딩은 기본 SGT 도메인으로 전송됩니다.

인바운드 SGT 도메인 규칙 추가:

1. Work Centers(작업 센터) > TrustSec > SXP > Inbound & Outbound SGT Domain Rules(인바운드 및 아웃바운드 SGT 도메인 규칙)를 선택합니다.
2. Inbound SGT Domain Rules(인바운드 SGT 도메인 규칙) 탭에서 Add Inbound Rule(인바운드 규칙 추가)을 클릭합니다.
3. Rule Settings(규칙 설정) 영역에 규칙 이름을 입력합니다.
4. Enabled를 클릭합니다.
5. Destination 드롭다운 목록에서 바인딩을 수신해야 하는 SGT 도메인을 선택합니다. 도메인을 추가하려면 Create SGT Domain(SGT 도메인 생성)을 사용합니다.
6. Rule Configuration(규칙 컨피그레이션) 영역에서 SGT Name(SGT 이름), Source(소스), IP Address(IP 주소)와 같은 특성이나 사전에 추가된 모든 vCenter 특성(예: os)으로 조건을 작성합니다. 필요에 따라 AND 및 OR로 조건을 결합합니다.
7. Add(추가)를 클릭한 다음 Save(저장)를 클릭합니다.

아웃바운드 SGT 도메인 규칙 추가:

1. 같은 페이지에서 Outbound SGT Domain Rules(아웃바운드 SGT 도메인 규칙) 탭을 열고 Add Outbound Rule(아웃바운드 규칙 추가)을 클릭합니다.
2. 규칙 이름을 입력하고 Enabled를 클릭합니다.
3. Destination 드롭다운 목록에서 SGT를 전송해야 하는 대상을 선택합니다.
4. Rule Configuration(규칙 컨피그레이션) 영역에서 SGT Domains(SGT 도메인), SGT Name(SGT 이름) 또는 IP Address(IP 주소)에서 조건을 작성합니다.
5. 선택적으로, Contract Configuration(계약 컨피그레이션) 영역에서 공유 보안 그룹에 대해 Consumed and Provided contracts(소비된 계약 및 제공된 계약)를 할당합니다.
6. Add(추가)를 클릭한 다음 Save(저장)를 클릭합니다.

인바운드 및 아웃바운드 규칙을 추가 또는 수정하는 동안 일치하는 IP-SGT 바인딩을 검토하려면 Preview 옵션을 사용합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

연결 상태 확인

Work Centers(작업 센터) > TrustSec > Integrations(통합) > Workload Connectors(워크로드 커넥터)

) > Workload Connections(워크로드 연결)를 선택하고 vCenter 연결이 Connected(연결됨) 상태로 나열되어 있는지 확인합니다. 이 페이지에서 연결을 다시 연결, 일시 중단 또는 삭제할 수도 있습니다.

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)						

Connected(연결됨) 상태의 vCenter 커넥터, 수신된 SGT 바인딩 수, 동기화 간격 및 마지막 업데이트 시간을 보여 주는 Workload Connections(워크로드 연결) 페이지

분류 규칙이 작업 로드와 일치하기 전에 캡처가 수행되었으므로 Received SGT Bindings 열은 이 이미지에서 0을 읽습니다. Connected 상태와 0 바인딩 카운트는 Cisco ISE가 성공적으로 vCenter에 도달했지만 아직 어떤 것에도 SGT를 할당하지 않았음을 의미합니다. 규칙이 일치하면 이 열은 Cisco ISE에서 파생된 바인딩 수를 보고합니다.

보안 그룹 확인

Work Centers(작업 센터) > TrustSec > Components(구성 요소) > Security Groups(보안 그룹)를 선택하고 필요한 SGT가 있는지 확인합니다. 이 예에서는 Production_Servers SGT가 있는지 확인합니다.

IP-SGT 바인딩 확인

Work Centers(작업 센터) > TrustSec > SXP > SGT Bindings(SGT 바인딩)를 선택하고 워크로드 IP 주소가 올바른 SGT에 바인딩되었는지, 올바른 소스와 적용된 분류 규칙을 사용하여 확인합니다.

워크로드 라이브 세션 확인

Operations(운영) > Workloads(워크로드) > Live Session(라이브 세션)을 선택하면 Workload Live Sessions(워크로드 라이브 세션) 페이지가 열립니다. 라이브 세션은 기본 PAN(정책 관리 노드)에서

만 볼 수 있습니다. 이 페이지에서는 커넥터 유형별로 세션을 필터링하고, 열을 표시하고, 숨기고, 재정렬하고, 결과를 정렬하고, 필터를 저장하고, 데이터를 CSV 또는 PDF 형식으로 내보낼 수 있습니다.

Workload Live Sessions

Export 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	192.168.10.72	---	---	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

Workload Live Sessions(워크로드 라이브 세션) 테이블에는 학습된 워크로드당 하나의 행이 나열되며, Initiated(시작) 타임스탬프, SGT Bindings(SGT 바인딩) IP 주소, empty SGT Name(빈 SGT 이름), Secondary SGTs(보조 SGT), Destinations(대상) 열, Source(소스) 연결 이름 LAB_VCenter 및 Inbound SGT Domain Rules(인바운드 SGT 도메인 규칙) 및 SGT Domains(SGT 도메인) 링크는 Default Filter(기본 필터) 및 default(기본값)를 읽습니다.



참고: 이 캡처는 이 예에서 데이터를 전달하는 열로 잘립니다. Outbound SGT Domain Rules(아웃바운드 SGT 도메인 규칙) 및 Workload Classification Rules(워크로드 분류 규칙) 열은 가시 영역의 오른쪽으로 계속 이어지며, 그 나머지의 ACI 관련 열이 그러하듯이 모든 행에서 비어 있습니다. 이 페이지는 커넥터 컨피그레이션 페이지보다 나중 Lab 세션에서 캡처되었으므로 시작된 타임스탬프가 이전에 [작업 로드 연결] 페이지에 표시된 [마지막으로 업데이트된 시간]과 일치하지 않습니다.

각 행은 Cisco ISE가 커넥터에서 학습한 하나의 워크로드를 나타냅니다. 다음 열을 사용하여 통합을 확인합니다.

열	확인 사항
시작됨	Cisco ISE가 세션을 학습한 시간입니다. 최근 타임스탬프는 커넥터가 폴링되고 있음을 확인합니다.

열	확인 사항
SGT 바인딩	Cisco ISE가 vCenter에서 수신한 워크로드 IP 주소입니다.
소스	세션을 보고한 작업 로드 연결입니다. 데이터가 어느 커넥터에서 왔는지 확인합니다.
인바운드 SGT 도메인 규칙 및 SGT 도메인	세션에 적용된 도메인 규칙 및 SGT 도메인. 일치하는 규칙을 보려면 링크를 선택합니다.
SGT 이름, 보조 SGT 및 워크로드 분류 규칙	워크로드에 할당된 SGT 및 이를 할당한 규칙입니다. 분류 규칙이 일치하지 않는 워크로드의 경우 이러한 열은 비어 있습니다.

페이지의 오른쪽 위 모서리에 있는 Refresh, Show 및 Within 컨트롤을 잘린 영역의 오른쪽에 사용하여 새로 고침 간격, 레코드 수 및 시간 창을 설정합니다.

이 이미지에서 SGT Bindings(SGT 바인딩) 열은 완전히 채워지며, SGT Name(SGT 이름) 및 Secondary SGT는 모든 행에서 비어 있습니다. 이는 분류 규칙이 일치하기 전에 캡처가 생성되었기 때문입니다. 잘린 영역 외부에 있는 Workload Classification Rules 열은 같은 이유로 비어 있습니다. 이 조합은 그 자체로 유용한 진단입니다. 커넥터가 vCenter에서 워크로드를 올바르게 검색하고 있으며 문제가 연결이 아닌 규칙 조건에 있음을 확인합니다. 해당 단계의 주의에 설명된 대로 3단계로 돌아가 Context Visibility가 보고하는 속성 값에 대한 일치 값을 확인합니다.

Context Visibility에서 워크로드 가시성 확인

 버전 요구 사항: Workload Connector Endpoints 대시보드는 Cisco ISE 3.5 Patch 3에서 계속 사용할 수 있습니다. Cisco ISE 3.4에서는 이전 섹션에서 설명한 Workload Live Sessions 페이지를 사용합니다.

Cisco ISE는 Context Visibility 내에서 전용 워크로드 커넥터 엔드포인트 대시보드를 제공합니다. 작업 로드 커넥터에서 수집한 엔드포인트 특성 데이터를 필터링 가능한 단일 보기로 수집, 분석 및 보고합니다.

뷰를 열려면 다음을 수행합니다.

1. Cisco ISE GUI에서 Context Visibility(상황 가시성) > Endpoints(엔드포인트)를 선택합니다.
2. Workload Connector Endpoints(워크로드 커넥터 엔드포인트) 탭을 엽니다. 탭 스트립에 탭이 표시되지 않으면 자세히를 클릭합니다.
3. Connector 드롭다운 목록에서 엔드포인트를 검토할 워크로드 연결을 선택합니다.

이 창에는 작업 로드 커넥터에서 가져오는 엔드포인트 특성 데이터가 나열됩니다. 각 행은 IP

Address, sourceType 및 Connector Name을 기준으로 엔드포인트를 식별합니다.

Workload Connector Endpoints

Rows/Page 25 1 / 1 > > | Go 23 Total Rows

Connector - LAB_VCenter

This window lists the endpoint attribute data that is fetched from Workload Connectors. Click 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
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

Context Visibility(컨텍스트 가시성) 아래의 Workload Connector Endpoints(워크로드 커넥터 엔드포인트) 보기에서는 IP 주소, 소스 유형 및 커넥터 이름별로 vCenter 워크로드 엔드포인트를 나열하며, Connector(커넥터) 드롭다운 목록은 LAB_VCenter, Export(내보내기) 옵션, Rows/Page(행/페이지) 및 pagination(페이지 매기기) 컨트롤로 설정되고 총 23개의 행이 포함됩니다.

이 보기에서 다음을 수행할 수 있습니다.

- 목록을 필터링합니다. IP 주소, 소스 유형 또는 커넥터 이름으로 결과를 좁히려면 열 헤더 아래의 필터 행을 사용합니다. 필터는 가산적이므로 적용하는 각 값은 결과 세트를 더 자세히 정의합니다.
- 결과를 한 페이지씩 살펴봅니다. 행/페이지 컨트롤과 페이지 매기기 화살표를 사용하여 페이지 크기를 변경하고 페이지 사이를 이동할 수 있습니다. 총 엔드포인트 수가 화살표 오른쪽에 나타나며, 여기에는 23개의 총 행으로 표시됩니다.
- 데이터 내보내기 Export(내보내기)를 클릭하여 나열된 엔드포인트 데이터를 다운로드합니다.
- 엔드포인트 검사 엔드포인트의 IP 주소를 클릭하여 Details(세부사항) 슬라이드인 창을 엽니다.

Details(세부 정보) 창에는 선택한 엔드포인트에 대해 Cisco ISE가 보유하는 모든 특성이 나열됩니다. Download(다운로드)를 클릭하여 특성 세부사항을 저장하거나 Cancel(취소)을 클릭하여 창을 닫습니다.

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

Cisco ISE가 해당 가상 머신에 대해 수집한 vCenter 속성의 ATTRIBUTES 목록과 Cancel 및 Download 컨트롤을 포함하는 커넥터 이름 및 엔드포인트 주소 위의 세부사항이라는 제목의 선택한 워크로드 엔드포인트에 대한 세부 정보 슬라이드 인 창

이 창은 LAB_VCenter_192.168.10.1로 표시된 작업 로드 연결 이름 및 엔드포인트 주소로 식별됩니다. vCenter 작업 로드 엔드포인트의 경우 특성에는 vCenter에서 학습된 가상 머신 속성(예: Power, VM-Name, host, macAddress, network, os, uuid, vmid 및 vmtype)과 커넥터 메타데이터(correlationId, source, ipAddress, connectorType 및 SourceType)이 포함됩니다. 사전에 추가한 사용자 지정 vCenter 태그도 여기에 표시됩니다.

이 창은 분류 규칙이 일치해야 하는 값에 대한 신뢰할 수 있는 소스이며, 먼저 이 창을 선택하면 이 워크플로에서 가장 일반적인 오류가 방지됩니다. 이 그림에서 os는 CentOS 4/5(64비트)를 읽는데, 이는 Equals(같음) 조건이 재현해야 하는 완전한 문자열입니다. CentOS와 같은 짧은 형식을 가정하기보다는 3단계에서 규칙을 작성하기 전에 여기서 값을 읽어보십시오.



참고: 각 엔드포인트에 대해 최대 50개의 특성이 표시됩니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

일반적인 문제

증상	가능한 원인	작업
커넥터 설정 중 연결 테스트 실패	하나 이상의 연결 세부 정보가 잘못되었거나 필수 구성 요소가 충족되지 않았습니다.	FQDN 또는 IP 주소를 확인하고 인증서 SAN과 일치하는지 확인합니다. 사용자 이름 및 비밀번호를 확인하고, 인증서 검증 설정을 검토하고, 프록시 바이패스 및 시간 동기화 사전 요구 사항이 충족되는지 확인합니다.
커넥터가 만들어졌지만 데이터를	Cisco ISE는 public.ecr.aws에 연결할 수 없습니다.	프록시 또는 방화벽이 이 URL에 대한 TCP 포트 443의 HTTPS 트래픽

증상	가능한 원인	작업
가져오지 않음		을 허용하는지 확인합니다.
워크로드는 가져 오지만 SGT는 할당되지 않으며 수신된 SGT 바 인딩은 0으로 유지됩니다.	분류 규칙 조건이 실제 특성 값과 일치하지 않습니다. CentOS 4/5(64비트) 대신 CentOS와 같은 부분 값에 대해 테스트된 Equals 조건이 가장 일반적인 원인입니다	Context Visibility에서 Details 창을 열고, 정확한 특성 값을 읽고, 규칙 조건을 수정하거나 연산자를 Contains로 변경합니다. 이 오류는 자동으로 발생합니다. 커넥터 자체가 정상이므로 경보가 울리지 않습니다.
연결이 일시 중단 상태로 이동	연결과 연결된 모든 SGT가 삭제되었습니다.	필수 SGT를 다시 생성하고 연결을 다시 설정합니다. 연결이 일시 중단되는 동안 관련 SXP 바인딩 및 MnT 세션 데이터가 제거됩니다.
PSN을 다시 시작한 후 연결 세부 정보가 없습니다.	세션 데이터가 다시 채워지지 않았습니다.	연결을 일시 중단한 다음 다시 연결합니다.

디버그 로그 사용

Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug Profile Configuration(디버그 프로파일 컨피그레이션)에서 PAN, SXP 및 pxGrid 노드에서 Workload Connector 구성 요소의 디버그 로그 심각도를 DEBUG로 설정합니다.

이러한 로그 파일은 /opt/CSCOCpm/logs에서 사용할 수 있습니다.

로그 파일	콘텐츠
workloads.log	워크로드 커넥터 작업.
workload-conn/*.log	연결당 로그
api-service.log	API 서비스 활동.
ise-psc.log	Cisco ISE 정책 서비스 활동.
pxgriddirect-service.log	pxGrid 직접 서비스 활동
sxp_appserver/sxp.log을 참조하십시오.	SXP 바인딩 배포입니다.

알람

Cisco ISE는 vCenter 및 기타 클라우드 커넥터에 대해 다음 경보를 생성합니다.

경보	발생 시간
작업 로드 연결 생성 /연결 실패	복원, 프로모션 또는 HA 이벤트, 업그레이드와 같은 이벤트가 발생한 후 커넥터 생성이 실패합니다.
작업 로드 연결 삭제 실패	커넥터 삭제에 실패했습니다.
작업 로드 연결 서비스 오류	다른 관련 서비스 오류가 발생했습니다.

관련 정보

- [Cisco ISE 공통 정책 및 워크로드 커넥터](#)
- [Cisco ISE 필수 인터넷 URL](#)
- [Cisco ISE 3.5 관리자 가이드](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.