

Configurar a integração do ISE Workload Connector com o VMware vCenter

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Cisco ISE](#)

[VMware vCenter](#)

[Conectividade](#)

[Certificados](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Termos principais](#)

[Espaços Reservados Usados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 1. Adicionar a conexão da carga de trabalho do vCenter](#)

[Etapa 2. Adicionar atributos do vCenter ao dicionário \(opcional\)](#)

[Etapa 3. Classificar cargas de trabalho em SGTs](#)

[Etapa 4. Ligações de Rota com Regras de Domínio SGT de Entrada e Saída](#)

[Verificar](#)

[Verifique o status da conexão](#)

[Verificar os Grupos de Segurança](#)

[Verifique as associações IP-SGT](#)

[Verificar as Sessões ao Vivo da Carga de Trabalho](#)

[Verificar a Visibilidade da Carga de Trabalho na Visibilidade do Contexto](#)

[Troubleshooting](#)

[Problemas comuns](#)

[Ativar logs de depuração](#)

[Alarmes](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o Cisco ISE Workload Connector for VMware vCenter para importar o contexto da carga de trabalho e aplicar a segmentação baseada em grupos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco ISE
- Administração do VMware vCenter
- Conceitos do Cisco TrustSec, incluindo Security Group Tags (SGTs), SGT Exchange Protocol (SXP) e pxGrid

Antes de adicionar uma conexão de carga de trabalho do vCenter, confirme se essas condições foram atendidas.

Cisco ISE

- o pxGrid está habilitado em pelo menos um nó na implantação.
- O SXP está habilitado em pelo menos um nó na implantação.

VMware vCenter

- Uma conta do vCenter com a permissão Somente Leitura está disponível. O conector executa somente operações de leitura.
- Os atributos ou marcas do vCenter a serem importados foram identificados. Este documento usa o atributo os como exemplo.

Conectividade

- Uma conexão de Internet estável está disponível para o Cisco ISE, pois o Cisco ISE pode acessar public.ecr.aws, que é exigido pelo recurso Conector de carga de trabalho. Se um servidor proxy ou firewall estiver no caminho, permita o tráfego HTTPS (porta TCP 443) entre o Cisco ISE e este URL. Se este URL não puder ser acessado, o Conector da Carga de Trabalho não funcionará conforme o esperado.
- Se um proxy for usado para acesso à Internet e o vCenter for implantado localmente, configure um desvio de proxy para o endereço IP do vCenter.

Certificados

- Se a validação do certificado for usada, o FQDN ou o endereço IP inserido para o vCenter deverá corresponder ao SAN (Nome Alternativo do Assunto) do certificado do ponto de extremidade do vCenter.
- O certificado raiz do vCenter deve estar disponível para importação no armazenamento de certificados confiáveis do Cisco ISE.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Identity Services Engine (ISE), versão 3.4, usado para os procedimentos de configuração e verificação do conector
- Cisco Identity Services Engine (ISE), Versão 3.5 Patch 3, usado somente para o procedimento de Visibilidade de Contexto
- VMware vCenter Server 8.0 atualização 3



Note: O painel Workload Connector Endpoints em Visibilidade de contexto requer o Cisco ISE 3.5 Patch 3 ou posterior, portanto, as duas imagens dessa seção foram capturadas nessa versão. Todos os outros procedimentos e imagens neste documento são provenientes do Cisco ISE 3.4.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os data centers modernos são dinâmicos. As máquinas virtuais (VMs) são criadas, movidas e desativadas continuamente, e seus endereços IP mudam com elas. As políticas de segurança que dependem de endereços IP estáticos ou sub-redes não podem acompanhar essa taxa de alteração, o que deixa lacunas na aplicação e na visibilidade.

O Cisco ISE resolve esse problema por meio da estrutura de política comum e seus conectores de carga de trabalho. Um conector de carga de trabalho estabelece uma conexão segura com um

data center ou uma plataforma de nuvem, importa o contexto das cargas de trabalho de aplicativos que são executadas lá, normaliza esse contexto em SGTs e compartilha o resultado com o restante da rede para que a política possa ser escrita contra ele.

O vCenter já descreve cada máquina virtual por meio de um conjunto de atributos, como o sistema operacional convidado, o grupo de portas ao qual ela se conecta e seu estado de energia. Os administradores do VMware ampliam essa descrição com tags personalizadas que transportam metadados como ambiente, camada de aplicativos, proprietário ou unidade de negócios. O vCenter Workload Connector importa ambos e os converte em SGTs. Isso gera três resultados:

- A política é baseada na carga de trabalho. Quando uma VM é movida ou é reendereçada, o SGT derivado do atributo permanece com ela, de modo que a segmentação continua a funcionar sem atualizações manuais.
- O contexto existente é reutilizado. O Cisco ISE consome os atributos e as tags que o vCenter já mantém, portanto, não é necessário um novo esquema de classificação.
- A segmentação é consistente. Os SGTs são distribuídos pela rede habilitada para TrustSec, portanto, a mesma política se aplica a todos os pontos de aplicação.

Este documento usa um único exemplo de execução em todo o documento. O atributo do sistema operacional relatado pelo vCenter para cada máquina virtual, que neste laboratório lê CentOS 4/5 (64 bits), é importado para o Cisco ISE e combinado com uma condição de endereço IP, para que as cargas de trabalho correspondentes sejam colocadas automaticamente em um grupo de segurança `Production_Servers`. Essas cargas de trabalho são segmentadas por associação de grupo, em vez de endereços IP rastreados manualmente. O mesmo procedimento se aplica a qualquer outro atributo ou marca personalizada que o vCenter expõe.

Termos principais



Note: O VMware ESXi não oferece suporte a marcas. Por esse motivo, somente o vCenter pode ser configurado como um conector de carga de trabalho. Os hosts ESXi autônomos não podem.

Termo	Definição
TrustSec	Tecnologia Cisco para segmentação baseada em grupos, na qual a política é escrita contra grupos em vez de endereços IP.
SGT (marcação de grupo de	Uma marca que representa um grupo, como Cargas de

Termo	Definição
segurança)	trabalho de produção, e serve como base para a aplicação de políticas.
SXP (SGT Exchange Protocol, Protocolo de troca de SGT)	O protocolo usado para distribuir associações IP-para-SGT para dispositivos de imposição.
pxGrid	A plataforma da Cisco usada para compartilhar contexto, como sessões e SGTs, entre o Cisco ISE e outros sistemas.
Política comum	A estrutura do Cisco ISE que se conecta a data centers e nuvens, normaliza seu contexto em SGTs e o compartilha entre domínios.
Conector da carga de trabalho	O componente Cisco ISE que se conecta ao vCenter, AWS, Azure, GCP ou ACI e importa o contexto da carga de trabalho.

Espaços Reservados Usados

Os valores entre colchetes são espaços reservados. Substitua-os pelos valores que se aplicam ao seu ambiente.

Espaço reservado	Descrição
[VCENTER_FQDN]	Nome de domínio totalmente qualificado do servidor vCenter.
[ENDEREÇO_IP_DO_VCENTER]	Endereço IP do servidor vCenter.
[NOME DO USUÁRIO]	Nome de usuário da conta somente leitura do vCenter.
[SENHA]	Senha da conta somente leitura do vCenter.
[SGT_NAME]	Nome da Tag de Grupo de Segurança atribuída por uma regra de classificação.
[NOME_VM]	Nome de uma máquina virtual no vCenter.

Espaço reservado	Descrição
[UUID_VM]	UUID de uma máquina virtual no vCenter.
[ID_VM]	Referência de objeto gerenciado do vCenter de uma máquina virtual.
[ID_DO_HOST]	Referência de objeto gerenciado do vCenter de um host ESXi.
[NOME_DA_REDE]	Nome do grupo de portas ou da rede do vCenter.

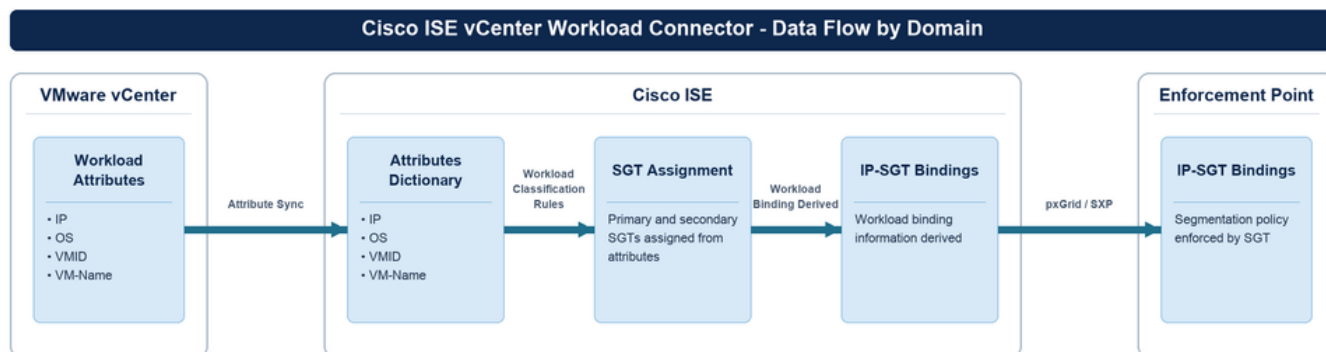
As imagens neste documento vêm de um laboratório que usa o nome de conexão da carga de trabalho LAB_vCenter, o endereço do vCenter 192.168.1.50 e a sub-rede da carga de trabalho 192.168.10.0/24. Substitua a nomeação e o endereçamento que se aplicam ao seu ambiente.

Configurar

Diagrama de Rede

A integração transforma os metadados do vCenter em uma política aplicável em cinco etapas:

1. O Cisco ISE vCenter Workload Connector lê os atributos e as marcas da carga de trabalho do vCenter.
2. Os atributos selecionados são adicionados ao Cisco ISE Attributes Dictionary para que possam ser referenciados em regras.
3. As Regras de Classificação de Carga de Trabalho avaliam esses atributos e designam um SGT principal e, opcionalmente, um ou mais SGTs secundários a cada carga de trabalho.
4. O Cisco ISE deriva as vinculações IP-para-SGT e as publica por meio do SXP e do pxGrid. As regras de domínio SGT de entrada e saída controlam quais domínios SGT recebem as associações e onde são compartilhados.
5. Os pontos de aplicação aplicam os SGTs para permitir ou negar tráfego.



O fluxo de dados do Cisco ISE vCenter Workload Connector passa por três domínios. O vCenter fornece atributos de carga de trabalho (IP, SO, VMID, VM-Name); O Cisco ISE os armazena no Dicionário de Atributos, aplica as Regras de Classificação de Carga de Trabalho para atribuir SGTs primários e secundários e deriva associações IP-SGT; as vinculações são compartilhadas por meio do pxGrid e do SXP com o Enforcement Point

Configurações

Etapa 1. Adicionar a conexão da carga de trabalho do vCenter

1. Na GUI do Cisco ISE, clique no ícone Menu e escolha Centros de trabalho > TrustSec > Integrações > Conectores de carga de trabalho > Conexões de carga de trabalho.
2. Clique em Add Connection.

Workload Connections

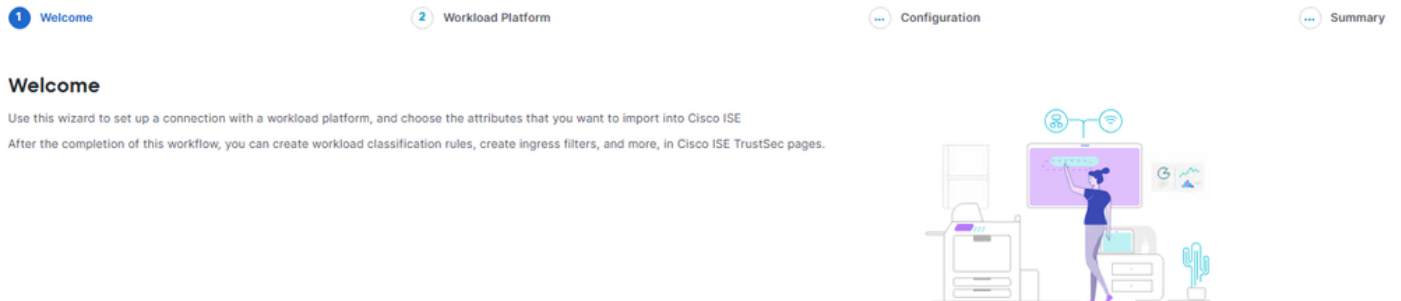
Create **workload classification rules** to assign SGTs to IP addresses and receive mappings. Manage **Inbound SGT domain rules** to define the SXP domains that must receive the mappings. Manage **Outbound SGT domain rules** to define the data shared from Cisco ISE to Cisco ACI.



No Workload Connected

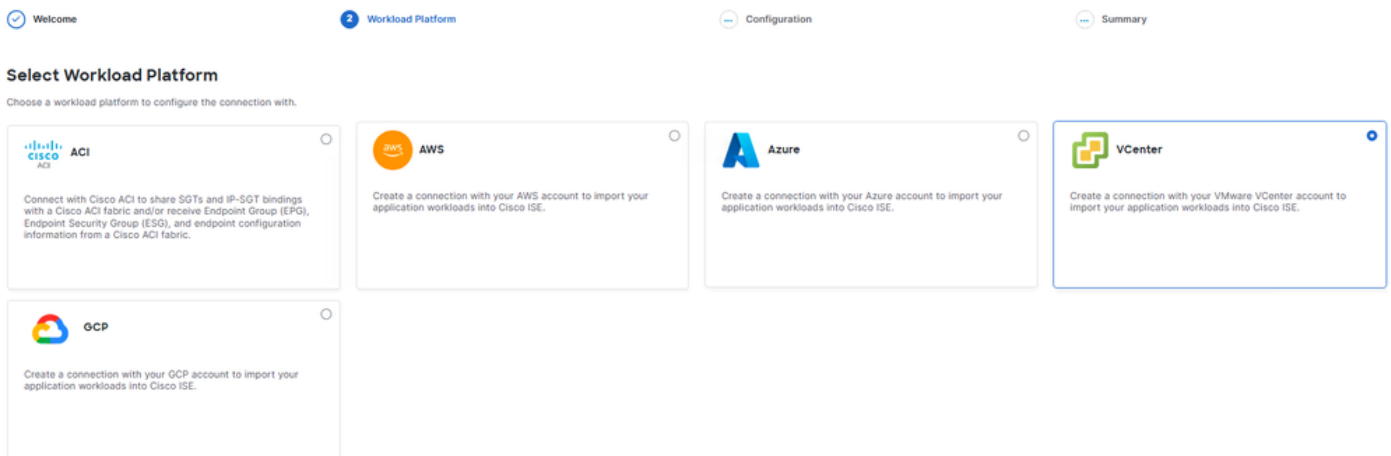
Add Connection

3. Clique em Vamos fazer isso.



Página Bem-vindo do assistente para conexão de carga de trabalho, mostrando os estágios Bem-vindo, Plataforma de Carga de Trabalho, Configuração e Resumo do assistente

4. Na página Selecionar plataforma de carga de trabalho, escolha vCenter e clique em Avançar.



Selecione a página Plataforma de carga de trabalho com a opção vCenter selecionada entre as plataformas ACI, AWS, Azure e GCP

5. Na página Criar conexão de carga de trabalho, o Cisco ISE verifica se os serviços do conector de carga de trabalho estão em execução antes de aceitar qualquer detalhe de

conexão.

Se os serviços ainda não estiverem em execução, a página informará que os Serviços do Conector de Carga de Trabalho não estão em execução.

Create Workload Connection

Checking Prerequisites

Workload Connector Services are not running

Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes

FQDN or IP address*

Hint

User*

Password*

☐ Validate vCenter certificate. ⓘ

Criar Conexão de Carga de Trabalho relatando que os serviços do Conector de Carga de Trabalho não estão em execução

Em seguida, o Cisco ISE inicia os serviços automaticamente e exibe o progresso.

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. [?](#)

Página Criar Conexão da Carga de Trabalho mostrando os serviços do Conector da Carga de Trabalho sendo iniciados

Aguarde até que a página informe que os Serviços do Conector de Carga de Trabalho estão em execução. Os campos de detalhes da conexão podem ser preenchidos somente após essa verificação ser bem-sucedida.

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.

Criar Conexão da Carga de Trabalho confirmando que os serviços do Conector da Carga de Trabalho estão em execução

6. Insira os detalhes da conexão:

Campo	Descrição
Nome da Conexão da Carga de Trabalho	Um nome exclusivo que usa letras, números e sublinhados. Máximo de 32 caracteres, sem espaços. Este exemplo usa LAB_VCenter.
Descrição	Uma descrição da conexão.
Intervalo de Sincronização	Com que frequência o Cisco ISE atualiza dados do vCenter. O intervalo válido é de 60 segundos a 7 dias. O padrão é 15 minutos. Intervalos menores atualizam os dados com mais frequência, mas podem afetar o desempenho.
FQDN ou	O nome do host ou endereço IP do vCenter, como [VCENTER_FQDN]

Campo	Descrição
endereço IP	ou [VCENTER_IP_ADDRESS]. Esse valor deve corresponder ao Nome Alternativo do Requerente do certificado do ponto de extremidade do vCenter.
Usuário	O nome de usuário da conta do vCenter, [USERNAME].
Senha	A senha da conta do vCenter, [PASSWORD].
Validar certificado do vCenter	Opcional. Valida o certificado e importa o certificado raiz do vCenter para o armazenamento de certificados confiáveis do Cisco ISE. Durante a importação, verifique também Trust para autenticação dos serviços Cisco. A validação de certificado é recomendada para ambientes de produção.

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. ⓘ

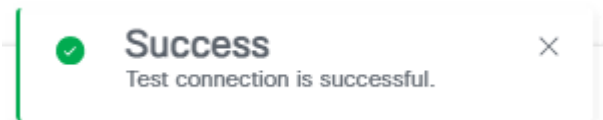
Página Criar conexão de carga de trabalho com os campos de detalhes de conexão do vCenter preenchidos e a caixa de seleção Validar certificado do vCenter marcada

Nesta imagem, o campo Usuário exibe um espaço reservado. Insira as credenciais que se aplicam ao seu ambiente.



Note: O Cisco ISE valida as informações inseridas. Se algum detalhe estiver incorreto, o Cisco ISE retorna o erro Test connection failed.

7. Clique em Next. O Cisco ISE testa a conexão e confirma o resultado com a mensagem Conexão de teste é bem-sucedida.



Notificação de êxito confirmando que a conexão de teste com o vCenter foi bem-sucedida

Notificação de êxito confirmando que a conexão de teste com o vCenter foi bem-sucedida

8. Na página Gerenciar atributos, escolha os atributos do vCenter a serem adicionados ao dicionário do Cisco ISE. Para este exemplo, certifique-se de que o atributo os esteja incluído. Em seguida, clique em Avançar.

- Para incluir todos os atributos aprendidos de uma vez, ative a alternância Incluir Tudo no Dicionário.
- Para renomear um atributo, edite o campo Nome do atributo no dicionário.
- Pelo menos um atributo deve ser adicionado para que você possa continuar.
- Nomes de atributo que contêm caracteres especiais, como ^, =, ", \, |, :, [ou] são inválidos e não podem ser adicionados.

☒ 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	--

Gerenciar atributos com a alternância Incluir tudo no dicionário ativada e os atributos vCenter aprendidos listados

Role a lista para examinar cada atributo que a conexão aprendeu do vCenter, como vmid, uuid, os, network, macAddress, VM-Name, host, Power e 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: 10 1 - 9 < 1 >

Página Gerenciar atributos rolada para mostrar a lista completa de atributos vCenter aprendidos e a contagem de registros

9. Na página Resumo, revise a configuração. Clique em Editar ao lado de qualquer seção para alterar seus valores.

✓ 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

Página de resumo mostrando a plataforma de carga de trabalho do V-CENTER selecionada e os atributos que estão incluídos no dicionário

10. Clique em Criar. O Cisco ISE confirma o resultado com a mensagem Connection successfully created.



Notificação de êxito confirmando que a conexão da carga de trabalho foi criada

O novo conector vCenter é exibido na página Conexões de carga de trabalho. O status é Connecting enquanto o Cisco ISE estabelece a sessão com o vCenter.

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)						

Página Conexões de carga de trabalho listando o novo conector do vCenter no estado Conectando

Etapa 2. Adicionar atributos do vCenter ao dicionário (opcional)

Conclua esta etapa apenas se desejar adicionar um atributo personalizado. Os atributos que você escolhe durante a etapa Manage Attributes são adicionados ao dicionário do vCenter automaticamente, de modo que a integração funciona sem nenhuma ação aqui. Os atributos de dicionário também podem ser gerenciados a qualquer momento após a criação da conexão:

1. Escolha Centros de trabalho > TrustSec > Integrações > Conectores de carga de trabalho.
2. Clique em Dicionário de Atributos.
3. Clique em Adicionar atributo.
4. Ative a alternância Incluir no dicionário.
5. No campo Atributo da Carga de Trabalho, informe o nome do atributo, como os.
6. No campo Nome do atributo no dicionário, digite o nome a ser exibido.
7. Click Save.

Observe este comportamento do dicionário:

- Um dicionário é criado por tipo de conexão. Todos os conectores do vCenter compartilham um único dicionário do vCenter.
- Os atributos não são removidos automaticamente quando uma conexão é excluída. Qualquer atributo que não esteja em uso pode ser excluído manualmente.
- Os atributos podem ser importados do provedor e os atributos que não estão presentes no

provedor podem ser adicionados manualmente.

Etapa 3. Classificar cargas de trabalho em SGTs

As regras de classificação de carga de trabalho avaliam os atributos da carga de trabalho, incluindo as marcas do vCenter que foram importadas e atribuem SGTs. Esta etapa fornece o valor de segmentação da integração.

A atribuição de SGT se comporta conforme descrito nestes itens:

- O SGT principal é marcado como Grupo de segurança no tópico de sessão do pxGrid e é usado para publicar mapeamentos de IP para SGT através do SXP.
- Os SGTs secundários estão incluídos no tópico da sessão do pxGrid como um array ordenado chamado Grupos de segurança secundários.
- Se várias regras corresponderem e atribuírem vários SGTs principais, apenas o primeiro SGT atribuído será tratado como principal. Os SGTs restantes se tornam secundários.

Para criar uma regra de classificação para este exemplo:

1. Escolha Centros de trabalho > TrustSec > Integrações > Classificação de carga de trabalho.
2. Clique em Adicionar regra de classificação.
3. Na área RULE SETTINGS, insira um Rule Name e defina Status como Enabled.
4. Na área AUTHORIZATION CONFIGURATION, na lista suspensa Primary SGT, escolha o SGT que a regra atribui, como [SGT_NAME]. Este exemplo atribui o SGT Production_Servers.
5. Como opção, na lista suspensa SGTs secundários (opcional), escolha um ou mais SGTs secundários.
6. Na área CONFIGURAÇÃO DE REGRA, crie a condição de correspondência. Na lista suspensa de atributos, escolha um atributo vCenter importado, como Vcenter - os, escolha o operador Equals e insira o valor a ser correspondido. Este exemplo corresponde a CentOS 4/5 (64 bits).
7. Para restringir ainda mais a regra, clique em Adicionar condição e combine as condições com AND ou OR. Este exemplo adiciona uma condição Endereço IP que usa o operador IP Equals para restringir a regra ao endereço de host único 192.168.10.33/32.
8. Opcionalmente, clique em Visualizar para revisar os detalhes do SGT e as cargas de trabalho correspondentes à regra.
9. Clique em Add.



Caution: O operador Equals requer o valor de atributo completo. O vCenter relata o sistema operacional convidado como uma sequência descritiva completa, como CentOS 4/5 (64 bits), não como um nome curto, como CentOS. Uma regra que testa Equals CentOS em relação a esse valor nunca corresponde e falha silenciosamente: o conector continua importando cargas de trabalho, mas nenhum SGT é atribuído. Confirme o valor exato em Visibilidade do Contexto antes de criar a regra, conforme descrito na seção Verificar, ou use um operador como Contém se quiser corresponder a uma família de sistemas operacionais convidados.

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

Página Adicionar regra de classificação atribuindo o SGT primário Production_Servers quando o atributo do sistema operacional vCenter for igual a CentOS 4/5 (64 bits) e o endereço IP for igual a 192.168.10.33/32

Repita essas etapas para cada grupo adicional de cargas de trabalho que deseja classificar e atribua um SGT principal diferente a cada regra.

Observe este comportamento de regra:

- As regras podem ser reordenadas arrastando e soltando. A ordem determina a prioridade.
- Uma nova regra ou uma regra duplicada pode ser inserida antes ou depois de uma regra existente.

- A regra de classificação padrão está sempre na parte inferior da lista, é desativada por padrão e mapeia para o SGT principal Desconhecido.
- Use a opção Preview para revisar os detalhes do SGT e as regras correspondentes antes de salvar.

Etapa 4. Ligações de Rota com Regras de Domínio SGT de Entrada e Saída

Os domínios SGT controlam quais partes da rede recebem ligações SGT específicas. Se nenhuma regra de entrada for definida, as associações recebidas dos conectores de carga de trabalho serão enviadas ao domínio SGT padrão.

Adicionar uma regra de domínio SGT de entrada:

1. Escolha Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules.
2. Na guia Inbound SGT Domain Rules, clique em Add Inbound Rule.
3. Na área Definições da regra, digite um nome de regra.
4. Clique em Enabled.
5. Na lista suspensa Destination, escolha os domínios SGT que devem receber as vinculações. Para adicionar um domínio, use Criar domínio SGT.
6. Na área Configuração de regra, crie a condição a partir de atributos como Nome SGT, Origem, Endereço IP ou qualquer atributo vCenter que tenha sido adicionado ao dicionário, como os. Combine as condições com AND e OR conforme necessário.
7. Clique em Adicionar e em Salvar.

Adicionar uma regra de domínio SGT de saída:

1. Na mesma página, abra a guia Outbound SGT Domain Rules e clique em Add Outbound Rule.
2. Insira um nome de regra e clique em Enabled.
3. Na lista suspensa Destination, escolha os destinos para os quais os SGTs devem ser enviados.
4. Na área Configuração de regra, crie a condição a partir de Domínios SGT, Nome SGT ou Endereço IP.
5. Como opção, na área Configuração do contrato, atribua contratos Consumidos e Fornecidos para os grupos de segurança compartilhados.
6. Clique em Adicionar e em Salvar.

Use a opção Preview para revisar as vinculações IP-SGT correspondentes enquanto adiciona ou edita regras de entrada e saída.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique o status da conexão

Escolha Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections e confirme se a conexão do vCenter está listada com o status Connected. Nessa página, você também pode reconectar, suspender ou excluir uma conexão.

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)

Página Conexões de Carga de Trabalho mostrando o conector do vCenter com um status Conectado, a contagem de vinculações SGT recebidas, o intervalo de sincronização e a hora da última atualização

A coluna Ligações SGT Recebidas lê 0 nesta imagem porque a captura foi feita antes que qualquer regra de classificação correspondesse a uma carga de trabalho. Um status Connected junto com uma contagem de ligação zero significa que o Cisco ISE alcançou o vCenter com sucesso, mas ainda não atribuiu um SGT a nada. Após a correspondência de uma regra, essa coluna relata o número de vinculações derivadas do Cisco ISE.

Verificar os Grupos de Segurança

Escolha Work Centers > TrustSec > Components > Security Groups e confirme se os SGTs esperados existem. Para este exemplo, confirme se o SGT Production_Servers existe.

Verifique as associações IP-SGT

Escolha Work Centers > TrustSec > SXP > SGT Bindings e confirme se os endereços IP da carga de trabalho estão vinculados aos SGTs corretos, com a origem correta e a regra de classificação aplicada.

Verificar as Sessões ao Vivo da Carga de Trabalho

Escolha Operations > Workloads > Live Session, que abrirá a página Workload Live Sessions. As sessões ao vivo podem ser exibidas apenas no Policy Administration Node (PAN) principal. Nesta página, as sessões podem ser filtradas por tipo de conector, colunas podem ser mostradas, ocultas e reorganizadas, resultados podem ser classificados, filtros podem ser salvos e dados podem ser exportados em formato CSV ou PDF.

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

Tabela Sessões ao Vivo de Carga de Trabalho listando uma linha por carga de trabalho aprendida, com o carimbo de data/hora Iniciado, o endereço IP das Ligações SGT, as colunas Nome SGT vazio, SGTs Secundários e Destinos, o nome da conexão de Origem LAB_VCenter e os links Regras de Domínio SGT de Entrada e Domínios SGT que leem o Filtro Padrão e o padrão



Note: Essa captura é cortada nas colunas que transportam dados neste exemplo. As colunas Outbound SGT Domain Rules e Workload Classification Rules continuam à

direita da área visível e estão vazias em todas as linhas, assim como as colunas específicas da ACI além delas. Esta página foi capturada em uma sessão de laboratório posterior às páginas de configuração do conector, portanto seus timestamps Iniciados não correspondem ao Horário da Última Atualização mostrado anteriormente na página Conexões de Carga de Trabalho.

Cada linha representa uma carga de trabalho que o Cisco ISE aprendeu de um conector. Use estas colunas para confirmar a integração:

Coluna	O que ele confirma
Iniciado	A hora em que o Cisco ISE aprendeu a sessão. Carimbos de data/hora recentes confirmam que o conector está fazendo polling.
Ligações SGT	O endereço IP da carga de trabalho que o Cisco ISE recebeu do vCenter.
Fonte	A conexão de carga de trabalho que relatou a sessão. Confirma de qual conector os dados vieram.
Regras de domínio SGT de entrada e domínios SGT	A regra de domínio e o domínio SGT que foram aplicados à sessão. Selecione um link para exibir a regra correspondente.
Nome SGT, SGTs secundários e regras de classificação de carga de trabalho	Os SGTs atribuídos à carga de trabalho e à regra que os atribuiu. Essas colunas permanecem vazias para cargas de trabalho que não correspondem a regras de classificação.

Use os controles Refresh, Show e Within no canto superior direito da página, à direita da área cortada, para definir o intervalo de atualização, a contagem de registros e a janela de tempo.

Nesta imagem, a coluna Ligações SGT é totalmente preenchida enquanto Nome SGT e SGTs Secundários estão vazios em cada linha, porque a captura foi feita antes de uma regra de classificação corresponder. A coluna Regras de Classificação de Carga de Trabalho, que fica fora da área cortada, está vazia pelo mesmo motivo. Esta combinação é um diagnóstico útil por si só: ele confirma que o conector está recuperando cargas de trabalho do vCenter corretamente e que o problema está nas condições da regra, e não na conexão. Ao vê-la, retorne à Etapa 3 e verifique os valores de correspondência em relação aos valores de atributo que a Visibilidade de Contexto relata, conforme descrito em Cuidado nessa etapa.

Verificar a Visibilidade da Carga de Trabalho na Visibilidade do Contexto

 **Requisito de versão:** O painel Workload Connector Endpoints está disponível no Cisco ISE 3.5 Patch 3 em diante. No Cisco ISE 3.4, use a página Workload Live Sessions descrita na seção anterior.

O Cisco ISE oferece um painel dedicado de endpoints do conector de carga de trabalho dentro da visibilidade de contexto. Ele coleta, analisa e relata os dados de atributos de endpoint coletados dos conectores de carga de trabalho em uma única exibição filtrável.

Para abrir a view:

1. Na GUI do Cisco ISE, escolha Visibilidade de contexto > Endpoints.
2. Abra a guia Endpoints do Conector de Carga de Trabalho. Se a guia não estiver visível na faixa de guias, clique em Mais.
3. Na lista suspensa Conector, escolha a conexão da carga de trabalho cujos pontos finais você deseja revisar.

A janela lista os dados de atributo de ponto final que são buscados dos conectores de carga de trabalho. Cada linha identifica um ponto final por Endereço IP, sourceType e Nome do Conector.

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

A exibição Pontos finais do conector de carga de trabalho em Visibilidade de contexto, listando os pontos finais da carga de trabalho do vCenter por endereço IP, tipo de origem e nome do conector, com a lista suspensa Conector definida como LAB_VCenter, a opção Exportar, os controles de Linhas/Página e paginação e uma contagem total de 23 linhas

Nessa exibição, você pode:

- Filtrar a lista. Use a linha de filtro abaixo dos cabeçalhos de coluna para restringir os resultados por endereço IP, tipo de origem ou nome do conector. Os filtros são aditivos, de modo que cada valor aplicado refina ainda mais o conjunto de resultados.
- Percorra os resultados. Use o controle Linhas/Página e as setas de paginação para alterar o tamanho da página e se mover entre as páginas. O número total de pontos finais aparece à direita das setas, mostradas aqui como 23 Total de Linhas.
- Exporte os dados. Clique em Exportar para fazer download dos dados de ponto final listados.
- Inspecione um endpoint. Clique no endereço IP de um endpoint para abrir o painel deslizante Detalhes.

O painel Detalhes lista todos os atributos que o Cisco ISE mantém para o endpoint selecionado. Clique em Download para salvar os detalhes do atributo ou clique em Cancelar para fechar o painel.

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

Painel deslizante Detalhes de um endpoint de carga de trabalho selecionado, intitulado Detalhes acima do nome do conector e do endereço do endpoint, com a lista ATRIBUTOS de propriedades do vCenter coletadas pelo Cisco ISE para essa máquina virtual e os controles Cancelar e Download

O painel é identificado pelo nome da conexão da carga de trabalho e o endereço do ponto final, mostrado aqui como LAB_VCenter_192.168.10.1. Para um ponto final da carga de trabalho do vCenter, os atributos incluem as propriedades da máquina virtual aprendidas do vCenter, como Power, VM-Name, host, macAddress, network, os, uuid, vmid e vmtype, juntamente com os metadados do conector correlationId, source, ipAddress, connectorType e SourceType. Qualquer marca personalizada do vCenter que você adicionou ao dicionário também aparece aqui.

Este painel é a fonte oficial dos valores que as regras de classificação devem corresponder, e verificá-lo primeiro evita a falha mais comum neste fluxo de trabalho. Nesta imagem, o sistema operacional lê CentOS 4/5 (64 bits), que é a string completa que uma condição Equals deve reproduzir. Leia o valor aqui antes de escrever a regra na Etapa 3, em vez de assumir um formulário curto como CentOS.



Note: Um máximo de 50 atributos é exibido para cada endpoint.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Problemas comuns

Sintoma	Causa provável	Ação
Falha no teste de conexão durante a configuração do conector	Um ou mais detalhes da conexão estão incorretos ou um pré-requisito não foi atendido	Verifique o FQDN ou o endereço IP e confirme se ele corresponde à SAN do certificado. Verifique o nome de usuário e a senha, revise a configuração de validação do certificado e

Sintoma	Causa provável	Ação
		confirme se os pré-requisitos de desvio de proxy e sincronização de tempo foram atendidos.
O conector é criado, mas nenhum dado é importado	O Cisco ISE não pode acessar public.ecr.aws	Confirme se o proxy ou firewall permite o tráfego HTTPS na porta TCP 443 para este URL.
As cargas de trabalho são importadas, mas nenhum SGT é atribuído, e as vinculações SGT recebidas permanecem em 0.	Uma condição da regra de classificação não corresponde ao valor real do atributo. Uma condição Equals testada em relação a um valor parcial, como CentOS em vez de CentOS 4/5 (64 bits), é a causa mais comum	Abra o painel Detalhes em Visibilidade de contexto, leia o valor exato do atributo e corrija a condição da regra ou altere o operador para Contém. Esta falha é silenciosa: nenhum alarme é acionado, pois o próprio conector está íntegro.
A conexão passa para um estado Suspenso	Todos os SGTs associados à conexão foram excluídos	Recrie os SGTs necessários e restabeleça a conexão. As associações SXP e os dados de sessão MnT relacionados são removidos enquanto a conexão é suspensa.
Detalhes da conexão estão faltando após uma reinicialização da PSN	Os dados da sessão não foram preenchidos novamente	Suspenda a conexão e reconecte-a.

Ativar logs de depuração

Defina a severidade do log de depuração para o componente Conector de Carga de Trabalho como DEBUG nos nós PAN, SXP e pxGrid de Operações > Solução de Problemas > Assistente de Depuração > Configuração do Perfil de Depuração.

Esses arquivos de log estão disponíveis em /opt/CSCOCpm/logs:

Arquivo de log	Conteúdo
cargas de trabalho.log	Operações do conector de carga de trabalho.

Arquivo de log	Conteúdo
workload-conn/*.log	Logs por conexão.
api-service.log	Atividade do serviço de API.
ise-psc.log	Atividade de serviço de política do Cisco ISE.
pxgriddirect-service.log	atividade de serviço do pxGrid Direct.
sxp_appserver/sxp.log	Distribuição de ligação SXP.

Alarmes

O Cisco ISE gera estes alarmes para o vCenter e outros conectores de nuvem:

Alarme	Gerado quando
Conexão da Carga de Trabalho - Criação/Conexão Malsucedida	A criação do conector falha após um evento, como uma restauração, uma promoção, um evento HA ou uma atualização.
Exclusão da Conexão da Carga de Trabalho Malsucedida	Falha na exclusão do conector.
Erro do Serviço de Conexão de Carga de Trabalho	Outra falha de serviço relacionada ocorre.

Informações Relacionadas

- [Política comum do Cisco ISE e conectores de carga de trabalho](#)
- [URLs da Internet necessárias para o Cisco ISE](#)
- [Guia do administrador do Cisco ISE 3.5](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.