

Configuración de la integración del conector de carga de trabajo ISE con VMware vCenter

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[ISE de Cisco](#)

[VMware vCenter](#)

[Conectividad](#)

[Certificados](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Términos clave](#)

[Marcadores de posición utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Paso 1. Agregar la conexión de carga de trabajo de vCenter](#)

[Paso 2. Agregar atributos de vCenter al diccionario \(opcional\)](#)

[Paso 3. Clasificar las cargas de trabajo en SGT](#)

[Paso 4. Enlaces de ruta con reglas de dominio SGT entrantes y salientes](#)

[Verificación](#)

[Verificar el estado de la conexión](#)

[Verifique los grupos de seguridad](#)

[Verificar los enlaces IP-SGT](#)

[Verificar las sesiones en directo de la carga de trabajo](#)

[Verificar visibilidad de carga de trabajo en visibilidad de contexto](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Habilitar registros de depuración](#)

[Alarmas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Cisco ISE Workload Connector para VMware vCenter para importar el contexto de carga de trabajo y aplicar la segmentación basada en grupos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración de Cisco ISE
- Administración de VMware vCenter
- Conceptos de Cisco TrustSec, incluidos Security Group Tags (SGT), SGT Exchange Protocol (SXP) y pxGrid

Antes de agregar una conexión de carga de trabajo de vCenter, confirme que se cumplen estas condiciones.

ISE de Cisco

- pxGrid está habilitado en al menos un nodo de la implementación.
- SXP está habilitado en al menos un nodo de la implementación.

VMware vCenter

- Hay disponible una cuenta de vCenter con el permiso Sólo lectura. El conector sólo realiza operaciones de lectura.
- Se han identificado los atributos o etiquetas de vCenter que se van a importar. Este documento utiliza el atributo os como ejemplo.

Conectividad

- Cisco ISE dispone de una conexión a Internet estable, ya que Cisco ISE puede alcanzar public.ecr.aws, que es necesaria para la función Conector de carga de trabajo. Si hay un servidor proxy o un firewall en la ruta, permita el tráfico HTTPS (puerto TCP 443) entre Cisco ISE y esta URL. Si no se puede acceder a esta URL, el conector de carga de trabajo no funciona correctamente.
- Si se utiliza un proxy para el acceso a Internet y vCenter se implementa en las instalaciones, configure un desvío de proxy para la dirección IP del vCenter.

Certificados

- Si se utiliza la validación de certificados, el FQDN o la dirección IP introducidos para vCenter deben coincidir con el nombre alternativo del sujeto (SAN) del certificado del terminal del vCenter.
- El certificado raíz de vCenter debe estar disponible para su importación en el almacén de certificados de confianza de Cisco ISE.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine (ISE), versión 3.4, utilizado para los procedimientos de verificación y configuración del conector
- Cisco Identity Services Engine (ISE), versión 3.5, parche 3, solo se utiliza para el procedimiento de visibilidad de contexto
- VMware vCenter Server 8.0 (actualización 3)



Nota: El panel de terminales del conector de carga de trabajo en Context Visibility requiere Cisco ISE 3.5 Patch 3 o posterior, por lo que las dos imágenes de esa sección se capturaron en esa versión. Todos los demás procedimientos e imágenes de este documento provienen de Cisco ISE 3.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los Data Centers modernos son dinámicos. Las máquinas virtuales (VM) se crean, mueven y retiran continuamente, y sus direcciones IP cambian con ellas. Las políticas de seguridad que se basan en subredes o direcciones IP estáticas no pueden seguir el ritmo de este cambio, lo que deja lagunas tanto en la aplicación como en la visibilidad.

Cisco ISE aborda este problema a través del marco de políticas comunes y sus conectores de

carga de trabajo. Un conector de carga de trabajo establece una conexión segura con un Data Center o una plataforma de nube, importa el contexto de las cargas de trabajo de las aplicaciones que se ejecutan en él, normaliza ese contexto en SGT y comparte el resultado con el resto de la red para que se pueda escribir una política en su contra.

vCenter ya describe todas las máquinas virtuales a través de un conjunto de atributos, como el sistema operativo invitado, el grupo de puertos al que se conecta y su estado de alimentación. Los administradores de VMware amplían esa descripción con etiquetas personalizadas que incluyen metadatos como el entorno, el nivel de aplicación, el propietario o la unidad empresarial. El conector de carga de trabajo de vCenter importa ambos y los convierte en SGT. Esto ofrece tres resultados:

- La política se basa en la carga de trabajo. Cuando una VM se mueve o se vuelve a direccionar, la SGT derivada de atributos permanece con ella, por lo que la segmentación sigue funcionando sin actualizaciones manuales.
- Se reutiliza el contexto existente. Cisco ISE utiliza los atributos y etiquetas que ya mantiene vCenter, por lo que no se requiere ningún nuevo esquema de clasificación.
- La segmentación es coherente. Las SGT se distribuyen a través de la red habilitada para TrustSec, por lo que se aplica la misma política en cada punto de aplicación.

En este documento se utiliza un solo ejemplo en ejecución. El atributo os del que informa vCenter para cada máquina virtual, que en este laboratorio lee CentOS 4/5 (64 bits), se importa a Cisco ISE y se combina con una condición de dirección IP, de modo que las cargas de trabajo coincidentes se colocan automáticamente en un grupo de seguridad de Production_Servers. Estas cargas de trabajo se segmentan por pertenencia a grupos en lugar de por direcciones IP de seguimiento manual. El mismo procedimiento se aplica a cualquier otro atributo o etiqueta personalizada que vCenter exponga.

Términos clave



Nota: VMware ESXi no admite etiquetas. Por este motivo, solo vCenter se puede configurar como conector de carga de trabajo. Los hosts de ESXi independientes no pueden.

Término	Definición
TrustSec	Tecnología de Cisco para la segmentación basada en grupos, en la que las políticas se escriben contra grupos en lugar de direcciones IP.

Término	Definición
SGT (Security Group Tag)	Etiqueta que representa un grupo, como Cargas de trabajo de producción, y sirve de base para la aplicación de políticas.
SXP (protocolo de intercambio SGT)	Protocolo utilizado para distribuir enlaces de IP a SGT a los dispositivos de aplicación.
pxGrid	La plataforma de Cisco solía compartir contexto, como sesiones y SGT, entre Cisco ISE y otros sistemas.
Política común	El marco de Cisco ISE, que se conecta a los Data Centers y las nubes, normaliza su contexto en SGT y lo comparte entre dominios.
Conector de carga de trabajo	El componente de Cisco ISE que se conecta a vCenter, AWS, Azure, GCP o ACI e importa el contexto de la carga de trabajo.

Marcadores de posición utilizados

Los valores entre corchetes son marcadores de posición. Sustitúyalos por los valores que se aplican a su entorno.

Marcador	Descripción
[VCENTER_FQDN]	Nombre de dominio completo del servidor vCenter.
[VCENTER_IP_ADDRESS]	Dirección IP del servidor vCenter.
[Nombre de usuario]	Nombre de usuario de la cuenta de solo lectura de vCenter.
[CONTRASEÑA]	Contraseña de la cuenta de solo lectura de vCenter.
[SGT_NAME]	Nombre de la etiqueta de grupo de seguridad asignada por una regla de clasificación.
[VM_NAME]	Nombre de una máquina virtual en vCenter.
[VM_UUID]	UUID de una máquina virtual en vCenter.

Marcador	Descripción
[VM_ID]	Referencia de objeto administrado de vCenter de una máquina virtual.
[HOST_ID]	Referencia de objeto administrado de vCenter de un host de ESXi.
[NETWORK_NAME]	Nombre del grupo de puertos o de la red del vCenter.

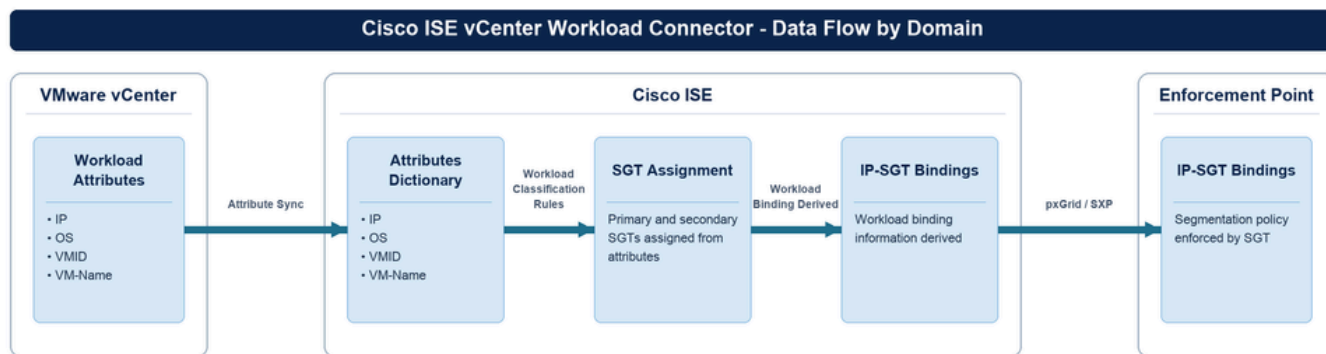
Las imágenes de este documento provienen de un laboratorio que utiliza el nombre de conexión de carga de trabajo LAB_vCenter, la dirección del vCenter 192.168.1.50 y la subred de carga de trabajo 192.168.10.0/24. Sustituya el nombre y la dirección que se aplican a su entorno.

Configurar

Diagrama de la red

La integración transforma los metadatos de vCenter en políticas aplicables en cinco etapas:

1. El conector de carga de trabajo de Cisco ISE vCenter lee las etiquetas y los atributos de la carga de trabajo de vCenter.
2. Los atributos seleccionados se agregan al diccionario de atributos de Cisco ISE para que se pueda hacer referencia a ellos en las reglas.
3. Las reglas de clasificación de cargas de trabajo evalúan estos atributos y asignan una SGT principal y, opcionalmente, una o varias SGT secundarias a cada carga de trabajo.
4. Cisco ISE deriva enlaces de IP a SGT y los publica a través de SXP y pxGrid. Las reglas de dominio SGT entrantes y salientes controlan qué dominios SGT reciben los enlaces y dónde se comparten.
5. Los puntos de aplicación aplican las SGT para permitir o denegar el tráfico.



Flujo de datos del conector de carga de trabajo de Cisco ISE vCenter en tres dominios. vCenter proporciona atributos de carga de trabajo (IP, SO, VMID, VM-Name); Cisco ISE los almacena en el diccionario de atributos, aplica reglas de clasificación de cargas de trabajo para asignar SGT principales y secundarias y deriva enlaces IP-SGT; los enlaces se comparten a través de pxGrid y SXP hasta el punto de aplicación

Configuraciones

Paso 1. Agregar la conexión de carga de trabajo de vCenter

1. En la GUI de Cisco ISE, haga clic en el icono Menu y elija Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections.
2. Haga clic en Agregar conexión.

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.

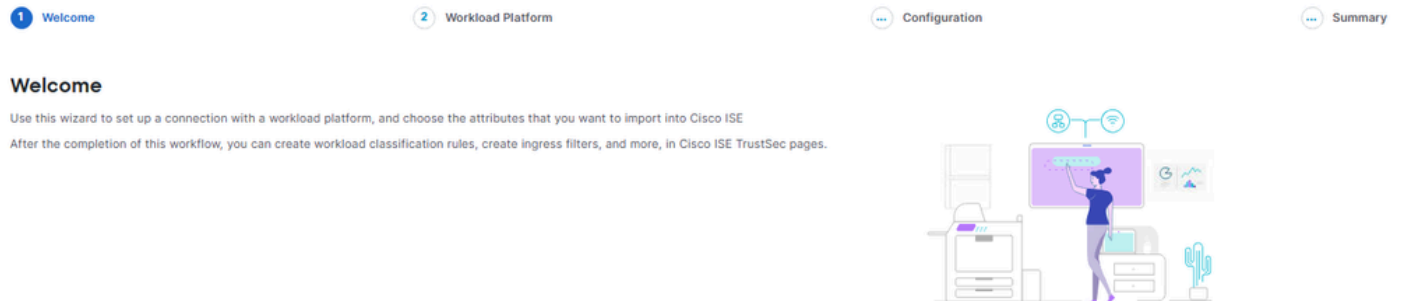


No Workload Connected

Add Connection

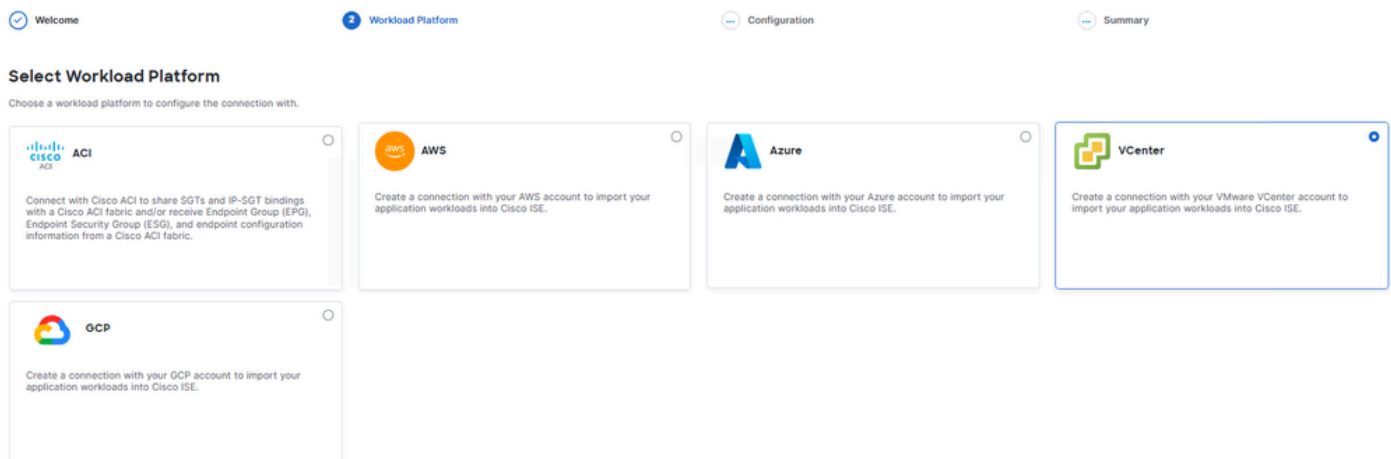
Página Conexiones de carga de trabajo sin conexiones configuradas, que muestra el botón Agregar conexión

3. Haga clic en Let's do it.



Asistente para la conexión de cargas de trabajo Página de bienvenida que muestra las fases Bienvenido, Plataforma de carga de trabajo, Configuración y Resumen del asistente

4. En la página Select Workload Platform, elija vCenter y, a continuación, haga clic en Next.



Seleccione la página Plataforma de carga de trabajo con la opción vCenter seleccionada entre las plataformas ACI, AWS, Azure y GCP

5. En la página Create Workload Connection, Cisco ISE comprueba si se están ejecutando los servicios de Conector de carga de trabajo antes de aceptar los detalles de conexión.

Si los servicios aún no se están ejecutando, la página informa de que no se están ejecutando los

servicios de Conector de carga de trabajo.

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. [?](#)

Página Crear Conexión de Carga de Trabajo que informa de que los servicios Conector de Carga de Trabajo no se están ejecutando

A continuación, Cisco ISE inicia los servicios automáticamente y muestra el progreso.

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 Crear Conexión de Carga de Trabajo que muestra el inicio de los servicios de Conector de Carga de Trabajo

Espere hasta que la página informe de que se están ejecutando los servicios de conector de carga de trabajo. Los campos de detalles de conexión sólo se pueden rellenar una vez que la comprobación se haya realizado correctamente.

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. ⓘ

Página Crear Conexión de Carga de Trabajo que confirma que los servicios Conector de Carga de Trabajo se están ejecutando

6. Introduzca los detalles de conexión:

Campo	Descripción
Nombre de conexión de carga de trabajo	Nombre único que utiliza letras, números y caracteres de subrayado. Máximo 32 caracteres, sin espacios. Este ejemplo utiliza LAB_VCenter.
Descripción	Una descripción de la conexión.
Intervalo de sincronización	Con qué frecuencia Cisco ISE actualiza los datos de vCenter. El intervalo válido es de 60 segundos a 7 días. El valor predeterminado es 15 minutos. Los intervalos más cortos actualizan los datos con más frecuencia, pero pueden afectar al rendimiento.
FQDN o dirección IP	El nombre de host o la dirección IP de vCenter, como [VCENTER_FQDN] o [VCENTER_IP_ADDRESS]. Este valor debe

Campo	Descripción
	coincidir con el nombre alternativo del sujeto del certificado del terminal del vCenter.
Usuario	El nombre de usuario de la cuenta del vCenter, [USERNAME].
Contraseña	La contraseña de la cuenta del vCenter, [PASSWORD].
Validar certificado de vCenter	Opcional. Valida el certificado e importa el certificado raíz de vCenter en el almacén de certificados de confianza de Cisco ISE. Durante la importación, compruebe también Trust para la autenticación de los servicios de Cisco. Se recomienda la validación de certificados para entornos de producción.

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. ⓘ

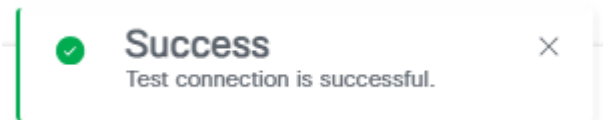
Página Crear conexión de carga de trabajo con los campos de detalle de conexión de vCenter completados y la casilla de verificación Validar certificado de vCenter activada

En esta imagen, el campo Usuario muestra un marcador de posición. Introduzca las credenciales que se aplican a su entorno.



Nota: Cisco ISE valida la información introducida. Si algún detalle es incorrecto, Cisco ISE devuelve el error Test connection failed.

7. Haga clic en Next (Siguiente). Cisco ISE prueba la conexión y confirma el resultado con el mensaje La conexión de prueba se ha realizado correctamente.



Notificación de éxito que confirma que la conexión de prueba con vCenter se ha realizado correctamente

Notificación de éxito que confirma que la conexión de prueba con vCenter se ha realizado correctamente

8. En la página Administrar atributos, elija los atributos de vCenter que desea agregar al diccionario de Cisco ISE. Para este ejemplo, asegúrese de incluir el atributo os. Luego haga clic en Next (Siguiente).

- Para incluir todos los atributos aprendidos a la vez, habilite la opción Include All in Dictionary.
- Para cambiar el nombre de un atributo, edite el campo Nombre del atributo en Diccionario.
- Se debe agregar al menos un atributo para poder continuar.
- Nombres de atributos que contienen caracteres especiales como ^, =, ", \, |, :, [, o] no son válidos y no se pueden agregar.

Include All in Dictionary

100

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	--

Página Administrar atributos con la opción Incluir todo en el diccionario activada y los atributos aprendidos del vCenter enumerados

Desplácese por la lista para revisar todos los atributos que la conexión aprendió de 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 >

La página Administrar atributos se desplazó para mostrar la lista completa de atributos aprendidos de vCenter y el recuento de registros

9. En la página Summary, revise la configuración. Haga clic en Editar junto a cualquier sección para cambiar sus 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 resumen que muestra la plataforma de carga de trabajo V-CENTER seleccionada y los atributos incluidos en el diccionario

10. Haga clic en Crear. Cisco ISE confirma el resultado con el mensaje Conexión creada correctamente.



Notificación de éxito que confirma que se ha creado la conexión de carga de trabajo

El nuevo conector vCenter aparece en la página Conexiones de carga de trabajo. El estado es Conectando mientras Cisco ISE establece la sesión con 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 Conexiones de carga de trabajo que enumera el nuevo conector vCenter en el estado Conexión

Paso 2. Agregar atributos de vCenter al diccionario (opcional)

Complete este paso sólo si desea agregar un atributo personalizado. Los atributos que elija durante el paso Administrar atributos se agregan automáticamente al diccionario vCenter, por lo que la integración funciona sin ninguna acción aquí. Los atributos de diccionario también se pueden administrar en cualquier momento después de crear la conexión:

1. Elija Centros de trabajo > TrustSec > Integraciones > Conectores de carga de trabajo.
2. Haga clic en Diccionario de atributos.
3. Haga clic en Agregar atributo.
4. Habilite la opción Include in Dictionary.
5. En el campo Atributo de Carga de Trabajo, introduzca el nombre del atributo, como os.
6. En el campo Nombre de Atributo en Diccionario, introduzca el nombre que se debe mostrar.
7. Click Save.

Tenga en cuenta este comportamiento de diccionario:

- Se crea un diccionario por tipo de conexión. Todos los conectores de vCenter comparten un único diccionario de vCenter.
- Los atributos no se eliminan automáticamente cuando se elimina una conexión. Cualquier atributo que no esté en uso se puede eliminar manualmente.
- Los atributos se pueden importar desde el proveedor y los atributos que no están presentes

en el proveedor se pueden agregar manualmente.

Paso 3. Clasificar las cargas de trabajo en SGT

Las reglas de clasificación de carga de trabajo evalúan los atributos de carga de trabajo, incluidas las etiquetas de vCenter que se han importado, y asignan SGT. Este paso proporciona el valor de segmentación de la integración.

La asignación de SGT se comporta como se describe en estos elementos:

- La SGT principal se marca como Security Group en el tema de sesión de pxGrid y se utiliza para publicar asignaciones de IP a SGT a través de SXP.
- Las SGT secundarias se incluyen en el tema de sesión de pxGrid como una matriz ordenada denominada Grupos de seguridad secundarios.
- Si varias reglas coinciden y asignan varias SGT principales, sólo la primera SGT asignada se trata como principal. Las SGT restantes pasan a ser secundarias.

Para crear una regla de clasificación para este ejemplo:

1. Elija Centros de trabajo > TrustSec > Integraciones > Clasificación de carga de trabajo.
2. Haga clic en Agregar regla de clasificación.
3. En el área CONFIGURACIÓN DE REGLA, ingrese un Nombre de regla y establezca Estado en Habilitado.
4. En el área AUTHORIZATION CONFIGURATION, en la lista desplegable Primary SGT, elija la SGT que asigna la regla, como [SGT_NAME]. En este ejemplo se asigna la SGT Production_Servers.
5. Opcionalmente, en la lista desplegable SGT secundarias (opcional), elija una o más SGT secundarias.
6. En el área CONFIGURACIÓN DE REGLA, genere la condición de coincidencia. En la lista desplegable de atributos, elija un atributo de vCenter importado, como Vcenter - os, elija el operador Equals e introduzca el valor con el que debe coincidir. Este ejemplo coincide con CentOS 4/5 (64-bit).
7. Para restringir aún más la regla, haga clic en Agregar condición y combine las condiciones con AND u OR. Este ejemplo agrega una condición IP Address que utiliza el operador IP Equals para restringir la regla a la dirección de host única 192.168.10.33/32.
8. De manera opcional, haga clic en Vista previa para revisar los detalles de SGT y las cargas de trabajo con las que coincide la regla.

9. Haga clic en Add (Agregar).



Precaución: El operador Equals requiere el valor de atributo completo. vCenter informa del sistema operativo invitado como una cadena descriptiva completa, como CentOS 4/5 (64 bits), no como un nombre corto, como CentOS. Una regla que compara Equals CentOS con ese valor nunca coincide y falla en silencio: el conector sigue importando cargas de trabajo, pero no se asigna ningún SGT. Confirme el valor exacto en Visibilidad del contexto antes de crear la regla, como se describe en la sección Verificar, o utilice un operador como Contiene si desea hacer coincidir una familia de sistemas operativos invitados.

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 Agregar regla de clasificación que asigna la SGT principal de Production_Servers cuando el atributo os de vCenter es igual a CentOS 4/5 (64 bits) y la dirección IP es igual a 192.168.10.33/32

Repita estos pasos para cada grupo adicional de cargas de trabajo que desee clasificar y asigne una SGT principal diferente a cada regla.

Tenga en cuenta este comportamiento de regla:

- Las reglas se pueden reordenar arrastrándolas y soltándolas. El orden determina la prioridad.
- Se puede insertar una nueva regla o una regla duplicada antes o después de una regla

existente.

- La regla de clasificación predeterminada siempre está al final de la lista, está desactivada de forma predeterminada y se asigna a la SGT Desconocida principal.
- Utilice la opción Preview para revisar los detalles de SGT y las reglas de coincidencia antes de guardar.

Paso 4. Enlaces de ruta con reglas de dominio SGT entrantes y salientes

Los dominios SGT controlan qué partes de la red reciben enlaces SGT específicos. Si no se definen reglas de entrada, los enlaces recibidos de los conectores de carga de trabajo se envían al dominio SGT predeterminado.

Agregar una regla de dominio SGT entrante:

1. Elija Centros de trabajo > TrustSec > SXP > Reglas de dominio SGT entrantes y salientes.
2. En la pestaña Reglas de dominio SGT entrantes, haga clic en Agregar regla entrante.
3. En el área Rule Settings, ingrese un nombre de regla.
4. Haga clic en Habilitado.
5. En la lista desplegable Destination, elija los dominios SGT que deben recibir los enlaces. Para agregar un dominio, utilice Create SGT Domain.
6. En el área Rule Configuration, genere la condición a partir de atributos como SGT Name, Source, IP Address o cualquier atributo vCenter agregado al diccionario, como OS. Combine las condiciones con AND y OR según sea necesario.
7. Haga clic en Agregar y, a continuación, haga clic en Guardar.

Agregar una regla de dominio SGT saliente:

1. En la misma página, abra la pestaña Reglas de dominio SGT salientes y haga clic en Agregar regla saliente.
2. Introduzca un nombre de regla y haga clic en Enabled.
3. En la lista desplegable Destination, elija los destinos a los que se deben enviar los SGT.
4. En el área Rule Configuration, cree la condición a partir de SGT Domains, SGT Name o IP Address.
5. De manera opcional, en el área Configuración de contratos, asigne contratos consumidos y proporcionados para los grupos de seguridad compartidos.
6. Haga clic en Agregar y, a continuación, haga clic en Guardar.

Utilice la opción Preview para revisar los enlaces IP-SGT coincidentes mientras agrega o edita reglas de entrada y de salida.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificar el estado de la conexión

Elija Centros de trabajo > TrustSec > Integraciones > Conectores de carga de trabajo > Conexiones de carga de trabajo y confirme que la conexión vCenter aparece con el estado Conectado. En esta página también puede volver a conectar, suspender o eliminar una conexión.

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 Conexiones de carga de trabajo que muestra el conector vCenter con el estado Conectado, el número de enlaces SGT recibidos, el intervalo de sincronización y la última hora actualizada

La columna Enlaces SGT recibidos lee 0 en esta imagen porque la captura se tomó antes de que cualquier regla de clasificación coincidiera con una carga de trabajo. El estado Connected junto con un recuento de enlaces cero significa que Cisco ISE ha alcanzado el vCenter correctamente, pero aún no ha asignado una SGT a nada. Después de que una regla coincida, esta columna informa del número de enlaces que Cisco ISE derivó.

Verifique los grupos de seguridad

Elija Centros de trabajo > TrustSec > Componentes > Grupos de seguridad y confirme que existen las SGT esperadas. Para este ejemplo, confirme que existe la SGT Production_Servers.

Verificar los enlaces IP-SGT

Elija Work Centers > TrustSec > SXP > SGT Bindings y confirme que las direcciones IP de carga de trabajo están enlazadas a las SGT correctas, con el origen correcto y la regla de clasificación aplicada.

Verificar las sesiones en directo de la carga de trabajo

Elija Operaciones > Cargas de trabajo > Sesión en directo, que abre la página Sesiones en directo de carga de trabajo. Las sesiones en directo solo se pueden ver en el nodo de administración de políticas (PAN) principal. En esta página, las sesiones se pueden filtrar por tipo de conector, las columnas se pueden mostrar, ocultar y reorganizar, los resultados se pueden ordenar, los filtros se pueden guardar y los datos se pueden exportar en formato CSV o PDF.

Workload Live Sessions

  Open To ▾

Initiated	SGT Bindings	SGT Name	Secondary SGTs	Source	Destinations	Inbound SGT Domain Rules	SGT Domains
✕	SGT Bindings	SGT Name	Secondary SGTs	Source	Destinations	Inbound SGT Domain Rules	SGT Domains
Aug 02, 2025 06:02 AM	192.168.10.72	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.120	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.5	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.75	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.2	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.102	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.226	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.241	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.72	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.101	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.254	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.243	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.242	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.1	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.74	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.11	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.33	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.80	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.76	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.245	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.68	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.227	---	---	LAB_VCenter	---	Default Filter	default
Aug 02, 2025 06:02 AM	192.168.10.13	---	---	LAB_VCenter	---	Default Filter	default

Tabla de sesiones en directo de carga de trabajo que enumera una fila por carga de trabajo aprendida, con el registro de hora de inicio, la dirección IP de enlaces de SGT, las columnas de nombre de SGT vacío, SGT secundarios y destinos, el nombre de conexión de origen LAB_VCenter y los enlaces Reglas de dominio de SGT entrante y Dominios SGT que leen Filtro predeterminado y predeterminado



Nota: Esta captura se recorta a las columnas que transportan los datos de este ejemplo.

Las columnas Reglas de dominio SGT salientes y Reglas de clasificación de carga de trabajo continúan a la derecha del área visible y están vacías en todas las filas, al igual que las columnas específicas de ACI situadas más allá de ellas. Esta página se capturó en una sesión de laboratorio posterior a las páginas de configuración del conector, por lo que sus marcas de hora de inicio no coinciden con la hora de la última actualización mostrada anteriormente en la página Conexiones de carga de trabajo.

Cada fila representa una carga de trabajo que Cisco ISE aprendió de un conector. Utilice estas columnas para confirmar la integración:

Columna	Lo que confirma
Iniciado	El momento en el que Cisco ISE aprendió la sesión. Las marcas de tiempo recientes confirman que el conector está sondeando.
Enlaces SGT	Dirección IP de carga de trabajo que Cisco ISE recibió de vCenter.
Fuente	La conexión de carga de trabajo que informó de la sesión. Confirma de qué conector proceden los datos.
Reglas de dominio SGT entrantes y dominios SGT	Regla de dominio y dominio SGT que se aplicaron a la sesión. Seleccione un vínculo para ver la regla coincidente.
Nombre de SGT, SGT secundarias y reglas de clasificación de cargas de trabajo	Las SGT asignadas a la carga de trabajo y la regla que las asignó. Estas columnas permanecen vacías para las cargas de trabajo con las que no coincide ninguna regla de clasificación.

Utilice los controles Refresh, Show y Within situados en la esquina superior derecha de la página, a la derecha del área recortada, para establecer el intervalo de actualización, el recuento de registros y la ventana de tiempo.

En esta imagen, la columna SGT Bindings está completamente llena mientras que SGT Name y SGT Secondary SGT están vacíos en cada fila, porque la captura se tomó antes de que una regla de clasificación coincidiera. La columna Reglas de clasificación de carga de trabajo, que se encuentra fuera del área recortada, está vacía por el mismo motivo. Esta combinación es un diagnóstico útil en sí mismo: confirma que el conector está recuperando correctamente las cargas de trabajo de vCenter y que el problema reside en las condiciones de la regla y no en la conexión. Cuando lo vea, vuelva al paso 3 y compare los valores de coincidencia con los valores de atributo que informa Visibilidad del contexto, como se describe en la sección Precaución de ese paso.

Verificar visibilidad de carga de trabajo en visibilidad de contexto

 **Requisito de versión:** El panel de terminales del conector de carga de trabajo está disponible a partir del parche 3 de Cisco ISE 3.5. En Cisco ISE 3.4, utilice la página Workload Live Sessions descrita en la sección anterior.

Cisco ISE proporciona un panel de terminales de conector de carga de trabajo dedicado dentro de la visibilidad del contexto. Recopila, analiza e informa de los datos de atributos de terminales recopilados de los conectores de carga de trabajo en una única vista filtrable.

Para abrir la vista:

1. En la GUI de Cisco ISE, elija Context Visibility > Endpoints.
2. Abra la pestaña Terminales Conector de carga de trabajo. Si la ficha no está visible en la franja de fichas, haga clic en Más.
3. En la lista desplegable Conector, elija la conexión de carga de trabajo cuyos terminales desea revisar.

La ventana enumera los datos de atributos de terminal que se obtienen de los conectores de carga de trabajo. Cada fila identifica un extremo por dirección IP, sourceType y nombre del conector.

Workload Connector Endpoints

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

Connector - LAB_VCenter or download the endpoint details.

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

Vista de extremos del conector de carga de trabajo en Visibilidad del contexto, que enumera los extremos de carga de trabajo de vCenter por dirección IP, tipo de origen y nombre del conector, con la lista desplegable Conector establecida en LAB_VCenter, la opción Exportar, los controles Filas/Página y paginación y un recuento de 23 filas en total

Desde esta vista, puede:

- Filtrar la lista. Utilice la fila de filtro situada debajo de los encabezados de columna para restringir los resultados por dirección IP, tipo de origen o nombre de conector. Los filtros son aditivos, por lo que cada valor que aplique refina aún más el conjunto de resultados.
- Consulte los resultados. Utilice el control Rows/Page y las flechas de paginación para cambiar el tamaño de página y desplazarse por las páginas. El número total de extremos aparece a la derecha de las flechas, que se muestran aquí como 23 filas totales.
- Exporte los datos. Haga clic en Exportar para descargar los datos de los terminales enumerados.
- Inspeccione un terminal. Haga clic en la dirección IP de un terminal para abrir el panel deslizable Detalles.

El panel Detalles muestra todos los atributos que Cisco ISE mantiene para el terminal seleccionado. Haga clic en Descargar para guardar los detalles del atributo, o haga clic en Cancelar para cerrar el panel.

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

Panel deslizable Detalles para un terminal de carga de trabajo seleccionado, titulado Detalles sobre el nombre del conector y la dirección del terminal, con la lista ATRIBUTOS de propiedades de vCenter que Cisco ISE recopiló para esa máquina virtual y los controles Cancelar y Descargar

El panel se identifica por el nombre de la conexión de carga de trabajo y la dirección del terminal, que se muestra aquí como LAB_VCenter_192.168.10.1. Para un extremo de carga de trabajo de vCenter, los atributos incluyen las propiedades de máquina virtual aprendidas de vCenter, como Power, VM-Name, host, macAddress, network, os, uuid, vmid y vmtype, junto con los metadatos del conector correlationId, source, ipAddress, connectorType y SourceType. Aquí también aparece cualquier etiqueta personalizada de vCenter que haya agregado al diccionario.

Este panel es el origen autorizado de los valores con los que deben coincidir las reglas de clasificación y, si lo activa primero, se evitará el error más común en este flujo de trabajo. En esta imagen, os lee CentOS 4/5 (64-bit), que es la cadena completa que una condición Equals debe reproducir. Lea el valor aquí antes de escribir la regla en el paso 3, en lugar de asumir un formato corto como CentOS.



Nota: Se muestra un máximo de 50 atributos para cada terminal.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Problemas comunes

Síntoma	Causa probable	Acción
Error en la conexión de prueba durante la configuración del conector	Uno o más detalles de conexión son incorrectos o no se cumple un requisito previo	Verifique el FQDN o la dirección IP y confirme que coincide con el certificado SAN. Verifique el nombre de usuario y la contraseña, revise la configuración de validación del certificado y

Síntoma	Causa probable	Acción
		confirme que se cumplen los requisitos previos de omisión del proxy y sincronización horaria.
Se crea el conector pero no se importan datos	Cisco ISE no puede alcanzar public.ecr.aws	Confirme que el proxy o el firewall permitan el tráfico HTTPS en el puerto TCP 443 a esta URL.
Las cargas de trabajo se importan pero no se asigna ningún SGT y los enlaces SGT recibidos permanecen en 0.	Una condición de regla de clasificación no coincide con el valor real del atributo. Una condición Equals probada contra un valor parcial, como CentOS en lugar de CentOS 4/5 (64 bits), es la causa más común	Abra el panel Detalles en Visibilidad de contexto, lea el valor de atributo exacto y corrija la condición de regla o cambie el operador a Contiene. Esta falla es silenciosa: no se genera ninguna alarma porque el conector en sí está en buen estado.
La conexión pasa al estado Suspendido	Se eliminaron todas las SGT asociadas a la conexión	Vuelva a crear las SGT necesarias y restablezca la conexión. Los enlaces SXP y los datos de sesión MnT relacionados se eliminan mientras se suspende la conexión.
Faltan los detalles de la conexión después de un reinicio de PSN	Los datos de la sesión no se rellenaron	Suspenda la conexión y, a continuación, vuelva a conectarla.

Habilitar registros de depuración

Establezca la gravedad del registro de depuración para el componente Conector de carga de trabajo en DEBUG en los nodos PAN, SXP y pxGrid desde Operaciones > Solución de problemas > Asistente de depuración > Configuración del perfil de depuración.

Estos archivos de registro están disponibles en /opt/CSCOcprm/logs:

Archivo de registro	Contenido
cargas de trabajo.log	Operaciones del conector de carga de trabajo.
load-conn/*.log	Registros por conexión.

Archivo de registro	Contenido
api-service.log	Actividad del servicio API.
ise-psc.log	Actividad del servicio de políticas de Cisco ISE.
pxgriddirect-service.log	actividad de servicio de pxGrid Direct.
sxp_appserver/sxp.log	Distribución de enlace SXP.

Alarmas

Cisco ISE genera estas alarmas para vCenter y otros conectores de nube:

Alarma	Se eleva cuando
Creación/conexión de la conexión de carga de trabajo incorrecta	La creación del conector falla después de un evento como una restauración, una promoción, un evento HA o una actualización.
Eliminación incorrecta de conexión de carga de trabajo	Error al eliminar el conector.
Error del servicio de conexión de carga de trabajo	Se produce otro error de servicio relacionado.

Información Relacionada

- [Conectores de carga de trabajo y políticas comunes de Cisco ISE](#)
- [URL de Internet necesarias para Cisco ISE](#)
- [Guía del administrador de Cisco ISE 3.5](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).