

Configurazione dell'integrazione di ISE Workload Connector con VMware vCenter

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Cisco ISE](#)

[VMware vCenter](#)

[Connettività](#)

[Certificati](#)

[Componenti usati](#)

[Premesse](#)

[Termini principali](#)

[Segnaposto utilizzati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Passaggio 1. Aggiunta della connessione al carico di lavoro vCenter](#)

[Passaggio 2. Aggiungere gli attributi vCenter al dizionario \(facoltativo\)](#)

[Passaggio 3. Classificazione dei carichi di lavoro nelle SGT](#)

[Passaggio 4. Regole di dominio SGT in entrata e in uscita per i binding di route](#)

[Verifica](#)

[Verifica dello stato della connessione](#)

[Verifica dei gruppi di sicurezza](#)

[Verificare i binding IP-SGT](#)

[Verifica delle sessioni attive del carico di lavoro](#)

[Verifica visibilità carico di lavoro in visibilità contesto](#)

[Risoluzione dei problemi](#)

[Problemi comuni](#)

[Abilita log di debug](#)

[Allarmi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Cisco ISE Workload Connector per VMware vCenter in modo da importare il contesto del carico di lavoro e applicare la

segmentazione basata su gruppi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione Cisco ISE
- Amministrazione di VMware vCenter
- Concetti di Cisco TrustSec, tra cui Security Group Tags (SGT), SGT Exchange Protocol (SXP) e pxGrid

Prima di aggiungere una connessione al carico di lavoro vCenter, verificare che queste condizioni siano soddisfatte.

Cisco ISE

- pxGrid è abilitato su almeno un nodo nella distribuzione.
- SXP è abilitato in almeno un nodo della distribuzione.

VMware vCenter

- È disponibile un account vCenter con autorizzazione Sola lettura. Il connettore esegue solo operazioni di lettura.
- Gli attributi o i tag di vCenter da importare sono stati identificati. Nel documento viene utilizzato l'attributo os come esempio.

Connettività

- Cisco ISE dispone di una connessione Internet stabile, in quanto Cisco ISE può raggiungere public.ecr.aws, richiesta dalla funzionalità Workload Connector. Se il percorso contiene un server proxy o un firewall, autorizzare il traffico HTTPS (porta TCP 443) tra Cisco ISE e questo URL. Se l'URL non è raggiungibile, il connettore del carico di lavoro non funziona come previsto.
- Se si utilizza un proxy per l'accesso a Internet e vCenter viene distribuito in locale, configurare

un bypass proxy per l'indirizzo IP di vCenter.

Certificati

- Se viene utilizzata la convalida del certificato, l'FQDN o l'indirizzo IP immesso per vCenter deve corrispondere al nome alternativo del soggetto (SAN) del certificato dell'endpoint vCenter.
- Il certificato radice vCenter deve essere disponibile per l'importazione nell'archivio dei certificati attendibili di Cisco ISE.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine (ISE), versione 3.4, utilizzato per le procedure di configurazione e verifica del connettore
- Cisco Identity Services Engine (ISE), versione 3.5, patch 3, utilizzata solo per la procedura di visibilità del contesto
- VMware vCenter Server 8.0 Aggiornamento 3



Nota: Il dashboard degli endpoint del connettore del carico di lavoro in Context Visibility richiede Cisco ISE 3.5 Patch 3 o versione successiva, quindi le due immagini in quella sezione sono state acquisite in quella release. Ogni altra procedura e immagine illustrata in questo documento proviene da Cisco ISE 3.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I moderni centri dati sono dinamici. Le macchine virtuali (VM) vengono create, spostate e ritirate continuamente e i relativi indirizzi IP cambiano. I criteri di sicurezza che si basano su indirizzi IP statici o subnet non possono tenere il passo con questa velocità di modifica, che lascia divari sia nell'applicazione che nella visibilità.

Cisco ISE risolve questo problema con il Common Policy Framework e i relativi connettori del carico di lavoro. Un connettore del carico di lavoro stabilisce una connessione sicura a un centro dati o a una piattaforma cloud, importa il contesto dei carichi di lavoro delle applicazioni che vi vengono eseguiti, normalizza tale contesto in SGT e condivide il risultato con il resto della rete in modo che i criteri possano essere scritti in base ad esso.

vCenter descrive già ogni macchina virtuale tramite una serie di attributi, ad esempio il sistema operativo guest, il gruppo di porte a cui si collega e il relativo stato di alimentazione. Gli amministratori VMware estendono tale descrizione con tag personalizzati che contengono metadati quali ambiente, livello applicazione, proprietario o business unit. vCenter Workload Connector importa entrambi e li converte in SGT. In questo modo si ottengono tre risultati:

- I criteri sono basati sul carico di lavoro. Quando una VM viene spostata o riindirizzata, il SGT derivato dall'attributo rimane con essa, quindi la segmentazione continua a funzionare senza aggiornamenti manuali.
- Il contesto esistente viene riutilizzato. Cisco ISE utilizza gli attributi e i tag già gestiti da vCenter, quindi non è necessario alcun nuovo schema di classificazione.
- La segmentazione è coerente. Poiché i servizi SGT vengono distribuiti sulla rete abilitata per TrustSec, lo stesso criterio viene applicato a ogni punto di imposizione.

In questo documento viene utilizzato un solo esempio in esecuzione in tutto. L'attributo os segnalato da vCenter per ciascuna macchina virtuale, che in questa esercitazione legge CentOS 4/5 (64 bit), viene importato in Cisco ISE e combinato con una condizione di indirizzo IP, in modo che i carichi di lavoro corrispondenti vengano inseriti automaticamente in un gruppo di sicurezza Production_Servers. Tali carichi di lavoro vengono quindi segmentati in base all'appartenenza ai gruppi anziché in base agli indirizzi IP rilevati manualmente. La stessa procedura si applica a qualsiasi altro attributo o tag personalizzato esposto da vCenter.

Termini principali



Nota: VMware ESXi non supporta i tag. Per questo motivo, solo vCenter può essere configurato come connettore del carico di lavoro. Gli host ESXi standalone non sono in grado di farlo.

Termine	Definizione
TrustSec	Tecnologia Cisco per la segmentazione basata su gruppi, in cui la policy viene scritta rispetto ai gruppi anziché agli indirizzi IP.

Termine	Definizione
SGT (tag gruppo di sicurezza)	Tag che rappresenta un gruppo, ad esempio i carichi di lavoro di produzione, e funge da base per l'applicazione dei criteri.
SXP (SGT Exchange Protocol)	Protocollo utilizzato per distribuire i binding da IP a SGT ai dispositivi di imposizione.
pxGrid	La piattaforma Cisco utilizzata per condividere il contesto, ad esempio sessioni e SGT, tra Cisco ISE e altri sistemi.
Politica comune	La struttura Cisco ISE, che si connette a data center e cloud, normalizza il loro contesto in SGT e lo condivide su più domini.
Connettore del carico di lavoro	Il componente Cisco ISE che si connette a vCenter, AWS, Azure, GCP o ACI e importa il contesto del carico di lavoro.

Segnaposto utilizzati

I valori racchiusi tra parentesi quadre sono segnaposto. Sostituirli con i valori validi per l'ambiente in uso.

Segnaposto	Descrizione
[VCENTER_FQDN]	Nome di dominio completo del server vCenter.
[VCENTER_IP_ADDRESS]	Indirizzo IP del server vCenter.
[USERNAME]	Nome utente account di sola lettura vCenter.
[PASSWORD]	Password account di sola lettura vCenter.
[NOME_SGT]	Nome del tag del gruppo di sicurezza assegnato da una regola di classificazione.
[NOME_VM]	Nome di una macchina virtuale in vCenter.
[UUID_VM]	UUID di una macchina virtuale in vCenter.

Segnaposto	Descrizione
[ID_VM]	Riferimento a oggetto gestito vCenter di una macchina virtuale.
[ID_HOST]	Riferimento a oggetti gestiti vCenter di un host ESXi.
[NOME_RETE]	Nome del gruppo di porte o della rete vCenter.

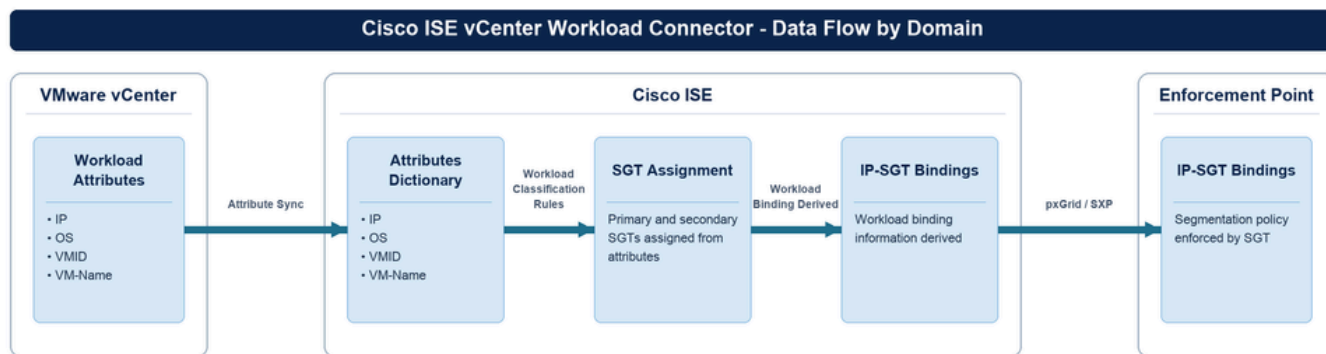
Le immagini di questo documento provengono da un'esercitazione che utilizza il nome della connessione al carico di lavoro LAB_VCenter, l'indirizzo vCenter 192.168.1.50 e la subnet del carico di lavoro 192.168.10.0/24. Sostituire i nomi e gli indirizzi applicabili all'ambiente.

Configurazione

Esempio di rete

L'integrazione trasforma i metadati di vCenter in regole applicabili in cinque fasi:

1. Cisco ISE vCenter Workload Connector legge gli attributi e i tag del carico di lavoro da vCenter.
2. Gli attributi selezionati vengono aggiunti al Cisco ISE Attributes Dictionary in modo che sia possibile farvi riferimento nelle regole.
3. Le regole di classificazione del carico di lavoro valutano questi attributi e assegnano un SGT principale e, facoltativamente, uno o più SGT secondari a ciascun carico di lavoro.
4. Cisco ISE deriva i binding IP-to-SGT e li pubblica tramite SXP e pxGrid. Le regole di dominio SGT in entrata e in uscita controllano quali domini SGT ricevono le associazioni e dove vengono condivisi.
5. I punti di applicazione applicano le SGT per autorizzare o negare il traffico.



Cisco ISE vCenter Workload Connector trasmette i dati su tre domini. vCenter fornisce gli attributi del carico di lavoro (IP, OS, VMID, VM-Name); Cisco ISE li memorizza nel dizionario attributi, applica le regole di classificazione del carico di lavoro per assegnare le SGT primarie e secondarie e deriva le associazioni IP-SGT; le associazioni vengono condivise tramite pxGrid e SXP al punto di applicazione Configurazioni

Passaggio 1. Aggiunta della connessione al carico di lavoro vCenter

1. Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu e scegliere Centri di lavoro > TrustSec > Integrazioni > Connettori del carico di lavoro > Connessioni al carico di lavoro.
2. Fare clic su Aggiungi connessione.

Workload Connections

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

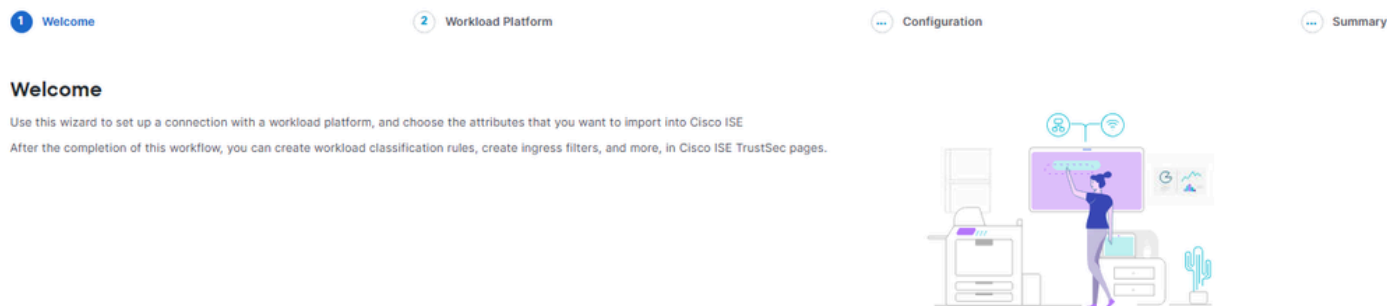


No Workload Connected

Add Connection

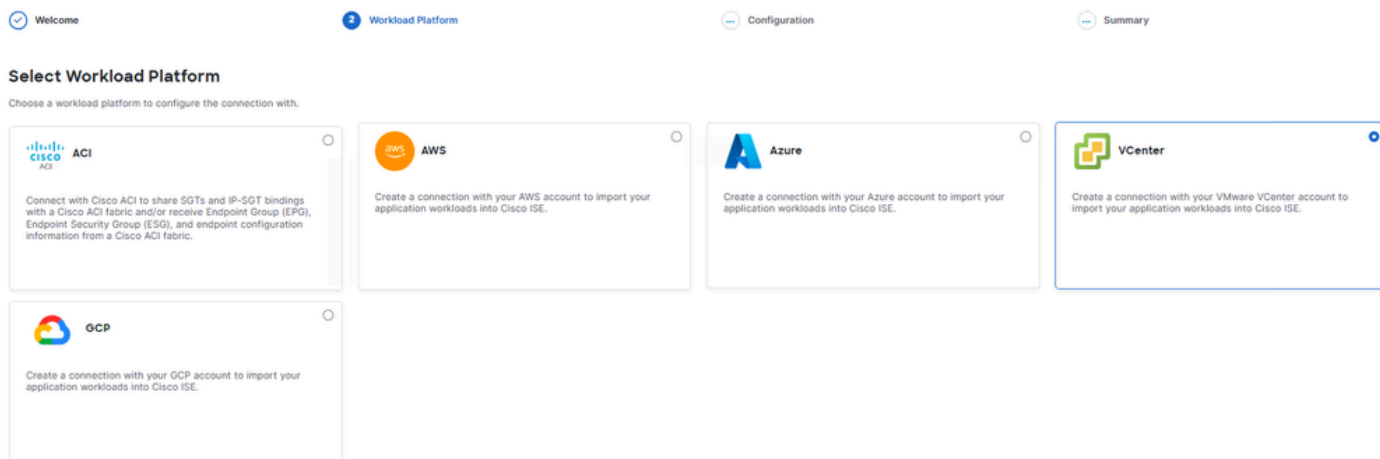
Pagina Connessioni del carico di lavoro senza connessioni configurate, con il pulsante Aggiungi connessione

3. Fare clic su Facciamolo.



Pagina iniziale della procedura guidata per la connessione al carico di lavoro, in cui sono mostrate le fasi Benvenuti, Piattaforma carico di lavoro, Configurazione e Riepilogo della procedura guidata

4. Nella pagina Seleziona piattaforma del carico di lavoro scegliere vCenter e quindi fare clic su Avanti.



Pagina Seleziona piattaforma del carico di lavoro con l'opzione vCenter selezionata tra le piattaforme ACI, AWS, Azure e GCP

5. Nella pagina Crea connessione al carico di lavoro, Cisco ISE controlla se i servizi Connettore carico di lavoro sono in esecuzione prima di accettare i dettagli della connessione.

Se i servizi non sono ancora in esecuzione, la pagina segnala che i servizi di Workload Connector non sono in esecuzione.

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. [?](#)

Pagina Crea connessione al carico di lavoro che segnala che i servizi di Workload Connector non sono in esecuzione

Cisco ISE avvia quindi i servizi automaticamente e visualizza lo stato di avanzamento.

Create Workload Connection

Checking Prerequisites

Starting the services



Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes



FQDN or IP address*

[Hint](#)

User*

Password*

☐ Validate vCenter certificate. [?](#)

Pagina Crea connessione carico di lavoro che mostra l'avvio dei servizi di Workload Connector

Attendere finché la pagina non segnala che i servizi di Workload Connector sono in esecuzione. I campi dei dettagli di connessione possono essere completati solo dopo il completamento di questo controllo.

Create Workload Connection

Workload Connector Services are running

Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes

▼

FQDN or IP address*

Hint

User*

Password*

☐ Validate vCenter certificate.

Pagina Crea connessione al carico di lavoro che conferma che i servizi di Workload Connector sono in esecuzione

6. Immettere i dettagli della connessione:

Campo	Descrizione
Nome connessione carico di lavoro	Nome univoco che utilizza lettere, numeri e caratteri di sottolineatura. Massimo 32 caratteri, senza spazi. Questo esempio utilizza LAB_VCenter.
Descrizione	Descrizione della connessione.
Intervallo di sincronizzazione	Frequenza con cui Cisco ISE aggiorna i dati da vCenter. L'intervallo valido è compreso tra 60 secondi e 7 giorni. L'impostazione predefinita è 15 minuti. Intervalli più brevi aggiornano i dati con maggiore frequenza, ma possono influire sulle prestazioni.
FQDN o indirizzo IP	Nome host o indirizzo IP di vCenter, ad esempio [VCENTER_FQDN] o [VCENTER_IP_ADDRESS]. Questo valore deve corrispondere al

Campo	Descrizione
	nome alternativo del soggetto del certificato dell'endpoint vCenter.
Utente	Il nome utente dell'account vCenter, [USERNAME].
Password	La password dell'account vCenter, [PASSWORD].
Convalida certificato vCenter	Facoltativo. Convalida il certificato e importa il certificato radice vCenter nell'archivio dei certificati protetti di Cisco ISE. Durante l'importazione, verificare anche l'attendibilità per l'autenticazione dei servizi Cisco. La convalida dei certificati è consigliata per gli ambienti di produzione.

Create Workload Connection

Workload Connector Services are running

Workload Connection Name*

LAB_VCenter

Non-editable after creation

Description

Sync Interval*

15

Minutes

FQDN or IP address*

192.168.1.50

Hint

User*

[USERNAME]

Password*

Show

☒ Validate vCenter certificate. ⓘ

Pagina Crea connessione carico di lavoro con i campi dei dettagli di connessione vCenter completati e la casella di controllo Convalida certificato vCenter selezionata

In questa immagine, il campo User visualizza un segnaposto. Immettere le credenziali applicabili all'ambiente.



Nota: Cisco ISE convalida le informazioni immesse. Se un dettaglio non è corretto, Cisco ISE restituirà l'errore Test della connessione non riuscito.

7. Fare clic su Next (Avanti). Cisco ISE verifica la connessione e conferma il risultato con il messaggio Test connessione riuscito.



Notifica di esito positivo che conferma che la connessione di prova a vCenter è stata completata

Notifica di esito positivo che conferma che la connessione di prova a vCenter è stata completata

8. Nella pagina Gestisci attributi, scegliere gli attributi vCenter da aggiungere al dizionario Cisco ISE. Per questo esempio, assicurarsi che l'attributo os sia incluso. Quindi fare clic su Avanti.

- Per includere contemporaneamente tutti gli attributi appresi, attivare l'interruttore Includi tutto nel dizionario.
- Per rinominare un attributo, modificare il campo Nome attributo nel dizionario.
- Per continuare, è necessario aggiungere almeno un attributo.
- Nomi di attributi che contengono caratteri speciali, ad esempio ^, =, ", \, |, :, [, o] non sono validi e non possono essere aggiunti.

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	--

Pagina Gestisci attributi con l'opzione Includi tutto nel dizionario abilitata e gli attributi vCenter appresi elencati

Scorrere l'elenco per esaminare tutti gli attributi appresi dalla connessione da vCenter, ad esempio 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 >

Scorrimento della pagina Gestisci attributi per visualizzare l'elenco completo degli attributi vCenter appresi e il conteggio dei record

9. Nella pagina Riepilogo esaminare la configurazione. Fare clic su Modifica accanto a una sezione per modificarne i valori.

✓ 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

Pagina di riepilogo che mostra la piattaforma di carico di lavoro V-CENTER selezionata e gli attributi inclusi nel dizionario

10. Fare clic su Crea. Cisco ISE conferma il risultato con il messaggio Connessione creata correttamente.



Notifica di riuscita che conferma la creazione della connessione al carico di lavoro

Il nuovo connettore vCenter viene visualizzato nella pagina Connessioni carico di lavoro. Lo stato è Connessione in corso mentre Cisco ISE stabilisce la sessione 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)						

Pagina Connessioni del carico di lavoro in cui è elencato il nuovo connettore vCenter nello stato Connessione

Passaggio 2. Aggiungere gli attributi vCenter al dizionario (facoltativo)

Completare questo passaggio solo se si desidera aggiungere un attributo personalizzato. Gli attributi scelti durante il passo Gestisci attributi vengono aggiunti automaticamente al dizionario vCenter, in modo che l'integrazione funzioni senza alcuna azione. Gli attributi del dizionario possono inoltre essere gestiti in qualsiasi momento dopo la creazione della connessione:

1. Scegliere Centri di lavoro > TrustSec > Integrazioni > Connettori del carico di lavoro.
2. Fare clic su Dizionario attributi (Attributes Dictionary).
3. Fare clic su Aggiungi attributo.
4. Attivare l'interruttore Includi nel dizionario.
5. Nel campo Attributo carico di lavoro immettere il nome dell'attributo, ad esempio os.
6. Nel campo Nome attributo nel dizionario, immettere il nome da visualizzare.
7. Fare clic su Save (Salva).

Si noti il seguente comportamento del dizionario:

- Viene creato un dizionario per ogni tipo di connessione. Tutti i connettori vCenter condividono un unico dizionario vCenter.
- Gli attributi non vengono rimossi automaticamente quando si elimina una connessione. Qualsiasi attributo non in uso può essere eliminato manualmente.
- Gli attributi possono essere importati dal provider e gli attributi non presenti nel provider

possono essere aggiunti manualmente.

Passaggio 3. Classificazione dei carichi di lavoro nelle SGT

Le regole di classificazione del carico di lavoro valutano gli attributi del carico di lavoro, inclusi i tag vCenter importati, e assegnano le SGT. Questa fase fornisce il valore di segmentazione dell'integrazione.

L'assegnazione SGT si comporta come descritto nei seguenti elementi:

- L'SGT primario è contrassegnato come Security Group nell'argomento della sessione pxGrid e viene utilizzato per pubblicare i mapping IP-SGT tramite SXP.
- Le SGT secondarie sono incluse nell'argomento della sessione pxGrid come un array ordinato denominato Secondary Security Groups.
- Se più regole corrispondono e assegnano più SGT primarie, solo la prima SGT assegnata viene considerata primaria. Le restanti SGT diventano secondarie.

Per creare una regola di classificazione per questo esempio:

1. Scegliere Centri di lavoro > TrustSec > Integrazioni > Classificazione carico di lavoro.
2. Fare clic su Aggiungi regola di classificazione.
3. Nell'area RULE SETTINGS, immettere un nome per la regola e impostare Status (Stato) su Enabled (Attivata).
4. Nell'area AUTHORIZATION CONFIGURATION (CONFIGURAZIONE AUTORIZZAZIONE), dall'elenco a discesa SGT principale, scegliere il SGT assegnato dalla regola, ad esempio [SGT_NAME]. In questo esempio viene assegnato il SGT Production_Servers.
5. Facoltativamente, dall'elenco a discesa SGT secondari (facoltativo) scegliere uno o più SGT secondari.
6. Nell'area RULE CONFIGURATION, creare la condizione di corrispondenza. Dall'elenco a discesa degli attributi, scegliere un attributo vCenter importato, ad esempio Vcenter - os, scegliere l'operatore Uguale a e immettere il valore corrispondente. In questo esempio viene restituito CentOS 4/5 (64 bit).
7. Per restringere ulteriormente la regola, fare clic su Aggiungi condizione e combinare le condizioni con AND o OR. In questo esempio viene aggiunta una condizione Indirizzo IP che utilizza l'operatore IP Equals per limitare la regola all'indirizzo host singolo 192.168.10.33/32.
8. Facoltativamente, fare clic su Anteprima per esaminare i dettagli SGT e i carichi di lavoro corrispondenti alla regola.

9. Fare clic su Add.



Attenzione: L'operatore Equals richiede il valore attributo completo. vCenter riporta il sistema operativo guest come stringa descrittiva completa, ad esempio CentOS 4/5 (64 bit), non come nome breve, ad esempio CentOS. Una regola che esegue il test di Equals CentOS in base a tale valore non corrisponde mai e ha esito negativo in modo invisibile all'utente: il connettore continua a importare carichi di lavoro, ma non viene assegnato alcun SGT. Confermare il valore esatto in Visibilità contesto prima di creare la regola, come descritto nella sezione Verifica, oppure utilizzare un operatore quale Contiene se si desidera che corrisponda a una famiglia di sistemi operativi guest.

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	

Pagina Aggiungi regola di classificazione in cui viene assegnato il server SGT primario Production_Servers quando l'attributo del sistema operativo vCenter è uguale a CentOS 4/5 (64 bit) e l'indirizzo IP è uguale a 192.168.10.33/32

Ripetere questi passaggi per ogni gruppo aggiuntivo di carichi di lavoro che si desidera classificare e assegnare un SGT primario diverso a ogni regola.

Si noti il comportamento di questa regola:

- Le regole possono essere riordinate mediante trascinamento. Ordine determina la priorità.
- È possibile inserire una nuova regola o una regola duplicata prima o dopo una regola

esistente.

- La regola di classificazione predefinita si trova sempre alla fine dell'elenco, è disabilitata per impostazione predefinita ed è mappata al SGT primario sconosciuto.
- Utilizzare l'opzione Preview per esaminare i dettagli SGT e le regole di abbinamento prima di salvare.

Passaggio 4. Regole di dominio SGT in entrata e in uscita per i binding di route

I domini SGT controllano le parti della rete che ricevono binding SGT specifici. Se non vengono definite regole in entrata, le associazioni ricevute dai connettori del carico di lavoro vengono inviate al dominio SGT predefinito.

Aggiungere una regola di dominio SGT in ingresso:

1. Scegliere Centri di lavoro > TrustSec > SXP > Regole di dominio SGT in entrata e in uscita.
2. Nella scheda Regole di dominio SGT in entrata fare clic su Aggiungi regola in entrata.
3. Nell'area Impostazioni regola immettere un nome per la regola.
4. Fare clic su Attivato.
5. Dall'elenco a discesa Destination (Destinazione), scegliere i domini SGT che devono ricevere i binding. Per aggiungere un dominio, utilizzare Crea dominio SGT.
6. Nell'area Configurazione regola creare la condizione da attributi quali Nome SGT, Origine, Indirizzo IP o da qualsiasi attributo vCenter aggiunto al dizionario, ad esempio os. Combinare le condizioni con AND e OR in base alle esigenze.
7. Fare clic su Add (Aggiungi), quindi su Save (Salva).

Aggiungere una regola di dominio SGT in uscita:

1. Nella stessa pagina aprire la scheda Regole di dominio SGT in uscita e fare clic su Aggiungi regola in uscita.
2. Immettere un nome per la regola e fare clic su Abilitato.
3. Dall'elenco a discesa Destination (Destinazione), selezionare le destinazioni alle quali devono essere inviate le SGT.
4. Nell'area Configurazione regole, creare la condizione da Domini SGT, Nome SGT o Indirizzo IP.
5. Facoltativamente, nell'area Configurazione contratto assegnare i contratti utilizzati e forniti per i gruppi di sicurezza condivisi.

6. Fare clic su Add (Aggiungi), quindi su Save (Salva).

Utilizzare l'opzione Preview per esaminare le associazioni IP-SGT corrispondenti durante l'aggiunta o la modifica di regole in entrata e in uscita.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica dello stato della connessione

Scegliere Centri di lavoro > TrustSec > Integrazioni > Connettori carico di lavoro > Connessioni carico di lavoro e confermare che la connessione vCenter sia elencata con lo stato Connesso. Da questa pagina è inoltre possibile riconnettersi, sospendere o eliminare una connessione.

Workload Connections

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

Q Search table						
0 Selected + Add Connection More Actions ▾						
☐	Workload Connection Name ↕	Platform	Status	Received SGT Bindings	Sync Interval	Last Updated Time
☐	LAB_VCenter	VCENTER	Connected	0	15 Minutes	Jul 24, 2025, 3:10 PM
1 Record(s)						

Pagina Connessioni del carico di lavoro che mostra il connettore vCenter con lo stato Connesso, il conteggio dei binding SGT ricevuti, l'intervallo di sincronizzazione e l'ora dell'ultimo aggiornamento

La colonna Received SGT Bindings legge 0 in questa immagine perché l'acquisizione è stata eseguita prima che qualsiasi regola di classificazione corrispondesse a un carico di lavoro. Se lo stato è Connesso e il numero di binding è pari a zero, Cisco ISE ha raggiunto vCenter correttamente ma non ha ancora assegnato un SGT. Dopo la corrispondenza di una regola, questa colonna indica il numero di binding derivati da Cisco ISE.

Verifica dei gruppi di sicurezza

Scegliere Centri di lavoro > TrustSec > Componenti > Gruppi di sicurezza e verificare che siano presenti le SGT previste. Per questo esempio, verificare che il SGT Production_Servers esista.

Verificare i binding IP-SGT

Scegliere Centri di lavoro > TrustSec > SXP > Associazioni SGT e confermare che gli indirizzi IP del carico di lavoro siano associati alle SGT corrette, con l'origine corretta e la regola di classificazione applicata.

Verifica delle sessioni attive del carico di lavoro

Scegliere Operazioni > Carichi di lavoro > Sessione live, che apre la pagina Carico di lavoro: sessioni attive. Le sessioni in tempo reale possono essere visualizzate solo nel PAN (Policy Administration Node) principale. In questa pagina è possibile filtrare le sessioni per tipo di connettore, visualizzare, nascondere e riordinare le colonne, ordinare i risultati, salvare i filtri ed esportare i dati in formato CSV o PDF.

Workload Live Sessions

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	192.168.10.79	---	---	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	192.168.10.220	---	---	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	192.168.10.191	---	---	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

Tabella Workload Live Sessions in cui viene elencata una riga per ogni carico di lavoro appreso, con le colonne Indicatore orario avviato, Indirizzo IP binding SGT, Nome SGT vuoto, SGT secondario e Destinazioni, Nome connessione di origine LAB_VCenter e Collegamenti Regole di dominio SGT in entrata e Domini SGT lettura Filtro predefinito e predefinito



Nota: Questa acquisizione viene ritagliata in base alle colonne che contengono i dati in questo esempio. Le colonne Regole di dominio SGT in uscita e Regole di classificazione del carico di lavoro continuano a destra dell'area visibile e sono vuote su ogni riga, come le colonne specifiche di ACI oltre ad esse. Questa pagina è stata acquisita in una sessione lab successiva rispetto alle pagine di configurazione del connettore, pertanto i relativi timestamp di Avvio non corrispondono all'ora dell'ultimo aggiornamento mostrata in precedenza nella pagina Connessioni del carico di lavoro.

Ogni riga rappresenta un carico di lavoro appreso da Cisco ISE da un connettore. Utilizzare queste colonne per confermare l'integrazione:

Colonna	Cosa conferma
Avviato	L'ora in cui Cisco ISE ha imparato la sessione. I timestamp recenti confermano che è in corso il polling del connettore.
Binding SGT	L'indirizzo IP del carico di lavoro che Cisco ISE ha ricevuto da vCenter.
Origine	Connessione al carico di lavoro che ha segnalato la sessione. Conferma da quale connettore provengono i dati.
Regole di dominio SGT in entrata e domini SGT	La regola di dominio e il dominio SGT applicati alla sessione. Selezionare un collegamento per visualizzare la regola corrispondente.
Nome SGT, SGT secondari e regole di classificazione del carico di lavoro	Le SGT assegnate al carico di lavoro e la regola che le ha assegnate. Queste colonne rimangono vuote per i carichi di lavoro a cui non corrisponde alcuna regola di classificazione.

Utilizzare i controlli Refresh, Show e Within nell'angolo superiore destro della pagina, a destra dell'area ritagliata, per impostare l'intervallo di aggiornamento, il conteggio dei record e la finestra temporale.

In questa immagine la colonna Associazioni SGT è completamente popolata mentre Nome SGT e SGT secondari sono vuoti su ogni riga, perché l'acquisizione è stata eseguita prima che una regola di classificazione corrispondesse. Per lo stesso motivo, la colonna Regole classificazione carico di lavoro, che si trova all'esterno dell'area ritagliata, è vuota. Questa combinazione è un'utile diagnostica a sé stante: verifica che il connettore recuperi correttamente i carichi di lavoro da vCenter e che il problema dipenda dalle condizioni della regola anziché dalla connessione.

Quando viene visualizzato, tornare al passo 3 e controllare i valori di corrispondenza rispetto ai valori degli attributi riportati nel rapporto Visibilità contesto, come descritto nell'attenzione di tale passo.

Verifica visibilità carico di lavoro in visibilità contesto

 **Requisito versione:** Il dashboard degli endpoint dei connettori del carico di lavoro è disponibile da Cisco ISE 3.5 Patch 3 in poi. Su Cisco ISE 3.4, utilizzare la pagina Workload Live Sessions descritta nella sezione precedente.

Cisco ISE fornisce un dashboard dedicato agli endpoint dei connettori del carico di lavoro all'interno di Context Visibility. Raccoglie, analizza e segnala i dati degli attributi dell'endpoint raccolti dai connettori del carico di lavoro in un'unica vista filtrabile.

Per aprire la vista:

1. Nell'interfaccia utente di Cisco ISE, scegliere Context Visibility > Endpoints.
2. Aprire la scheda Endpoint connettore carico di lavoro. Se la scheda non è visibile nell'elenco delle schede, fare clic su Altro.
3. Dall'elenco a discesa Connettore, scegliere la connessione al carico di lavoro di cui si desidera esaminare gli endpoint.

La finestra elenca i dati degli attributi dell'endpoint recuperati dai connettori del carico di lavoro. Ogni riga identifica un endpoint in base all'indirizzo IP, al tipo di origine e al nome del connettore.

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

Vista Endpoint connettore carico di lavoro in Visibilità contesto, con l'elenco a discesa Connettore impostato su LAB_VCenter,

l'opzione Esporta, i controlli Righe/Pagina e impaginazione e un conteggio di 23 righe totali

Da questa vista è possibile effettuare le seguenti operazioni:

- Filtrare l'elenco. Utilizzare la riga del filtro sotto le intestazioni di colonna per limitare i risultati in base all'indirizzo IP, al tipo di origine o al nome del connettore. Poiché i filtri si aggiungono, ogni valore applicato perfeziona ulteriormente l'insieme di risultati.
- Scorri i risultati. Utilizzare il controllo Rows/Page e le frecce di impaginazione per modificare le dimensioni della pagina e spostarsi tra le pagine. Il numero totale di punti finali viene visualizzato a destra delle frecce, indicato qui come 23 righe totali.
- Esportare i dati. Fare clic su Esporta per scaricare i dati dell'endpoint elencati.
- Ispezionare un endpoint. Fare clic sull'indirizzo IP di un endpoint per aprire il riquadro a tendina Dettagli.

Nel riquadro dei dettagli vengono elencati tutti gli attributi contenuti in Cisco ISE per l'endpoint selezionato. Fare clic su Download per salvare i dettagli dell'attributo oppure fare clic su Annulla per chiudere il riquadro.

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

Riquadro a tendina Dettagli per un endpoint del carico di lavoro selezionato, intitolato Dettagli sopra il nome del connettore e l'indirizzo dell'endpoint, con l'elenco ATTRIBUTI delle proprietà vCenter raccolte da Cisco ISE per la macchina virtuale e i controlli

Annulla e Scarica

Il riquadro è identificato dal nome della connessione al carico di lavoro e dall'indirizzo dell'endpoint, visualizzati qui come LAB_VCenter_192.168.10.1. Per un endpoint del carico di lavoro vCenter, gli attributi includono le proprietà della macchina virtuale apprese da vCenter, ad esempio Power, VM-Name, host, macAddress, network, os, uuid, vmid e vmtype, insieme ai metadati del connettore correlationId, source, ipAddress, connectorType e SourceType. In questa finestra vengono visualizzati anche tutti i tag vCenter personalizzati aggiunti al dizionario.

Questo riquadro è l'origine autorevole per i valori che le regole di classificazione devono corrispondere e la sua verifica consente di evitare gli errori più comuni nel flusso di lavoro. In questa immagine, il sistema operativo legge CentOS 4/5 (64 bit), che è la stringa completa che una condizione Equals deve riprodurre. Leggere il valore qui prima di scrivere la regola nel Passaggio 3, anziché assumere una forma breve come CentOS.



Nota: Per ogni endpoint vengono visualizzati al massimo 50 attributi.

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Problemi comuni

Sintomo	Probabile causa	Azione
Test della connessione non riuscito durante l'installazione del connettore	Uno o più dettagli di connessione non sono corretti o un prerequisito non è soddisfatto	Verificare l'FQDN o l'indirizzo IP e verificare che corrisponda alla SAN del certificato. Verificare il nome utente e la password, controllare l'impostazione di convalida del certificato e verificare che i prerequisiti per la

Sintomo	Probabile causa	Azione
		sincronizzazione dell'ora e il bypass del proxy siano soddisfatti.
Il connettore viene creato ma non vengono importati dati	Cisco ISE non può raggiungere public.ecr.aws	Confermare che il proxy o il firewall consenta il traffico HTTPS sulla porta TCP 443 su questo URL.
I carichi di lavoro vengono importati ma non viene assegnato alcun SGT e i binding SGT ricevuti rimangono impostati su 0.	Una condizione della regola di classificazione non corrisponde al valore effettivo dell'attributo. La causa più comune è una condizione Equals verificata rispetto a un valore parziale, ad esempio CentOS anziché CentOS 4/5 (64 bit)	Aprire il riquadro Dettagli in Visibilità contesto, leggere il valore esatto dell'attributo e correggere la condizione della regola oppure modificare l'operatore in Contiene. Questo errore non viene visualizzato: non viene generato alcun allarme in quanto il connettore è integro.
La connessione passa a uno stato Sospeso	Tutti i SGT associati alla connessione sono stati eliminati	Ricreare le SGT richieste e ristabilire la connessione. I binding SXP e i dati della sessione MnT correlati vengono rimossi mentre la connessione viene sospesa.
Dettagli di connessione mancanti dopo un riavvio PSN	Dati della sessione non ripopolati	Sospendere la connessione e riconnetterla.

Abilita log di debug

Impostare la gravità del log di debug per il componente Workload Connector su DEBUG sui nodi PAN, SXP e pxGrid da Operazioni > Risoluzione dei problemi > Procedura guidata di debug > Configurazione profilo di debug.

Questi file di registro sono disponibili in /opt/CSCOcpm/logs:

File di log	Contenuto
workloads.log	Operazioni connettore carico di lavoro.

File di log	Contenuto
workload-conn/*.log	Registri per connessione.
api-service.log	Attività servizio API.
ise-psc.log	Attività del servizio criteri Cisco ISE.
pxgriddirect-service.log	Attività di servizio pxGrid Direct.
sxp_appserver/sxp.log	Distribuzione binding SXP.

Allarmi

Cisco ISE genera questi allarmi per vCenter e altri connettori cloud:

Allarme	Generato quando
Creazione/connessione del carico di lavoro non riuscita	La creazione del connettore non riesce dopo un evento quale un ripristino, una promozione o un evento HA o un aggiornamento.
Eliminazione della connessione al carico di lavoro non riuscita	Eliminazione del connettore non riuscita.
Errore del servizio di connessione del carico di lavoro	Si verifica un altro errore di servizio correlato.

Informazioni correlate

- [Cisco ISE Common Policy e connettori per il carico di lavoro](#)
- [Cisco ISE - URL Internet richiesti](#)
- [Guida per l'amministratore di Cisco ISE 3.5](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).