

VMware vCenterとのISEワークロードコネクタ統合の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[Cisco ISE](#)

[VMware vCenter](#)

[接続](#)

[証明書](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[重要な用語](#)

[使用するプレースホルダ](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ステップ 1: vCenterワークロード接続の追加](#)

[ステップ 2ディクショナリへのvCenter属性の追加 \(オプション \)](#)

[ステップ 3ワークロードをSGTに分類](#)

[ステップ 4着信および発信SGTドメイン規則によるルートバインディング](#)

[確認](#)

[接続ステータスの確認](#)

[セキュリティグループの確認](#)

[IP-SGTバインディングの確認](#)

[ワークロードのライブセッションの確認](#)

[コンテキストの可視性でのワークロードの可視性の確認](#)

[トラブルシュート](#)

[一般的な問題](#)

[デバッグログの有効化](#)

[アラーム](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco ISE Workload Connector for VMware vCenterを設定して、ワークロードコンテキストをインポートし、グループベースのセグメンテーションを適用する方法につ

いて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ISEの管理
- VMware vCenterの管理
- セキュリティグループタグ(SGT)、SGT交換プロトコル(SXP)、pxGridを含むCisco TrustSecの概念

vCenterワークロード接続を追加する前に、次の条件が満たされていることを確認します。

Cisco ISE

- pxGridが展開の少なくとも1つのノードで有効になっています。
- SXPは、展開の少なくとも1つのノードで有効になっています。

VMware vCenter

- 読み取り専用権限を持つvCenterアカウントを使用できます。コネクタは読み取り操作のみを実行します。
- インポートするvCenter属性またはタグが特定されました。このドキュメントでは、例としてos属性を使用しています。

接続

- Cisco ISEはpublic.ecr.awsに到達できるため、Cisco ISEでは安定したインターネット接続を利用できます。これはワークロードコネクタ機能に必要です。プロキシサーバまたはファイアウォールがパスにある場合、Cisco ISEとこのURLの間のHTTPS (TCPポート443) トラフィックを許可します。このURLに到達できない場合、ワークロードコネクタは意図したとおりに機能しません。
- インターネットアクセスにプロキシが使用され、vCenterがオンプレミスで展開されている場合は、vCenter IPアドレスのプロキシバイパスを設定します。

証明書

- 証明書の検証を使用する場合、vCenterに入力するFQDNまたはIPアドレスは、vCenterエンドポイント証明書のサブジェクト代替名(SAN)と一致する必要があります。
- vCenterルート証明書が、Cisco ISEの信頼できる証明書ストアへのインポートに使用できる必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)、リリース3.4。コネクタの設定と検証手順に使用されます。
- Cisco Identity Services Engine(ISE)、リリース3.5パッチ3。コンテキストの可視性の手順にのみ使用されます。
- VMware vCenter Server 8.0アップデート3



注:Context VisibilityのワークロードコネクタエンドポイントダッシュボードにはCisco ISE 3.5 Patch 3以降が必要なため、このセクションの2つのイメージはそのリリースでキャプチャされました。このドキュメントの他のすべての手順とイメージは、Cisco ISE 3.4のものであります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

現代のデータセンターは動的です。仮想マシン(VM)は継続的に作成、移動、廃止され、IPアドレスも変更されます。スタティックIPアドレスまたはサブネットに依存するセキュリティポリシーは、この変化の速度に追いつけず、適用と可視性の両方にギャップが残ります。

Cisco ISEは、Common Policyフレームワークとワークロードコネクタを使用してこの問題に対処します。ワークロードコネクタは、データセンターまたはクラウドプラットフォームへの安全な接続を確立し、そこで実行されるアプリケーションワークロードのコンテキストをインポートし、そのコンテキストをSGTに正規化し、ポリシーを書き込むことができるように結果をネットワ

ークの他の部分と共有します。

vCenterでは、ゲストオペレーティングシステム、接続先のポートグループ、電源状態などの一連の属性を通じて、すべての仮想マシンがすでに説明されています。VMware管理者は、環境、アプリケーション層、所有者、ビジネス・ユニットなどのメタデータを保持するカスタム・タグを使用して、この説明を拡張します。vCenterワークロードコネクタは両方をインポートし、SGTに変換します。これにより、次の3つの成果が得られます。

- ・ポリシーはワークロードベースです。VMが移動または再アドレス指定されると、属性由来のSGTがVMに付随するため、セグメンテーションは手動で更新することなく継続して機能します。
- ・既存のコンテキストは再利用されます。Cisco ISEは、vCenterがすでに保持している属性とタグを使用するため、新しい分類スキームは必要ありません。
- ・セグメント化は一貫しています。SGTはTrustSec対応ネットワーク全体に分散されるため、すべての適用ポイントに同じポリシーが適用されます。

このドキュメントでは、全体を通して1つの実行例を使用します。vCenterが各仮想マシンについて報告するos属性(この実習ではCentOS 4/5 (64ビット) を読み取る)は、Cisco ISEにインポートされ、IPアドレス条件と組み合わせられます。これにより、一致するワークロードが自動的にProduction_Serversセキュリティグループに配置されます。これらのワークロードは、手動で追跡されるIPアドレスではなく、グループメンバーシップによってセグメント化されます。同じ手順は、vCenterが公開するその他の属性タグまたはカスタムタグにも適用されます。

重要な用語



注:VMware ESXiはタグをサポートしていません。このため、ワークロードコネクタとして設定できるのはvCenterだけです。スタンドアロンESXiホストは実行できません。

用語	定義
TrustSecの	IPアドレスではなくグループに対してポリシーが書き込まれる、グループベースのセグメンテーションに対応するシスコのテクノロジー。
SGT (セキュリティグループタグ)	Production Workloadsなどのグループを表し、ポリシーを適用するための基準として機能するタグ。
SXP (SGT交換プロトコル)	IPとSGT間のバインディングを適用デバイスに分散するために使用されるプロトコル。

用語	定義
pxGrid	セッションやSGTなどのコンテキストをCisco ISEと他のシステム間で共有するために使用されるシスコプラットフォーム。
共通ポリシー	データセンターやクラウドに接続し、コンテキストをSGTに標準化してドメイン間で共有するCisco ISEフレームワーク。
ワークロードコネクタ	vCenter、AWS、Azure、GCP、またはACIに接続し、ワークロードコンテキストをインポートするCisco ISEコンポーネント。

使用するプレースホルダ

角カッコ内の値はプレースホルダです。これらの値を、使用している環境に適用される値に置き換えてください。

プレースホルダ	説明
[VCENTER_FQDN]	vCenterサーバの完全修飾ドメイン名。
[VCENTER_IP_ADDRESS]	vCenterサーバのIPアドレス
[USERNAME]	vCenter読み取り専用アカウントユーザ名。
[PASSWORD]	vCenter読み取り専用アカウントパスワード。
[SGT_NAME]	分類規則によって割り当てられたセキュリティグループタグの名前。
[VM_NAME]	vCenterの仮想マシンの名前。
[VM_UUID]	vCenterの仮想マシンのUUID。
[VM_ID]	仮想マシンのvCenter管理オブジェクト参照。
[HOST_ID]	ESXiホストのvCenter管理対象オブジェクト参照。

プレースホルダ	説明
[NETWORK_NAME]	vCenterポートグループまたはネットワークの名前。

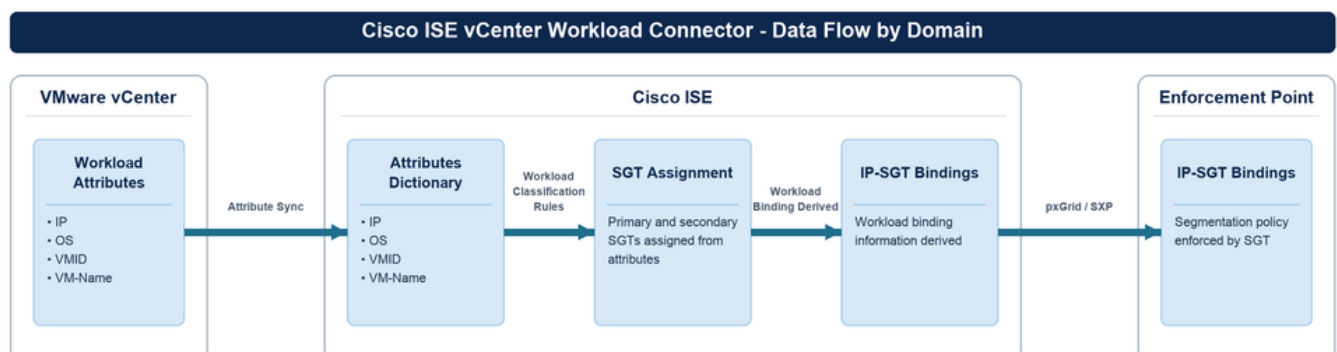
このドキュメントのイメージは、ワークロード接続名LAB_VCenter、vCenterアドレス192.168.1.50、ワークロードサブネット192.168.10.0/24を使用するラボのイメージです。環境に適用される名前とアドレスを置き換えます。

設定

ネットワーク図

この統合により、vCenterメタデータは次の5つの段階で実施可能なポリシーに変換されます。

1. Cisco ISE vCenterワークロードコネクタは、ワークロード属性とタグをvCenterから読み取ります。
2. 選択した属性がCisco ISE 属性ディクショナリに追加され、ルールで参照できるようになります。
3. ワークロード分類ルールは、これらの属性を評価し、プライマリSGTとオプションで1つ以上のセカンダリSGTを各ワークロードに割り当てます。
4. Cisco ISEはIPとSGTのバインディングを導出し、SXPおよびpxGridを介してバインディングを公開します。着信および発信SGTドメイン規則は、バインディングを受信するSGTドメインと、バインディングの共有場所を制御します。
5. エンフォースメントポイントは、SGTを適用してトラフィックを許可または拒否します。



3つのドメイン間のCisco ISE vCenterワークロードコネクタのデータフロー。
vCenterはワークロード属性(IP、OS、VMID、VM-Name)を提供します。Cisco ISEはワークロード属性を属性ディクショナリに格納し、ワークロード分類ルール

を適用してプライマリおよびセカンダリSGTを割り当て、IP-SGTバインディングを導出します。バインディングは、pxGridおよびSXPを介して適用してします
コンフィギュレーション

ステップ 1 : vCenterワークロード接続の追加

1. Cisco ISE GUIで、Menuアイコンをクリックし、Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connectionsの順に選択します。
2. Add Connectionをクリックします。

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

接続が構成されていない[ワークロード接続]ページで、[接続の追加]ボタンが表示されている

3. Let's do itをクリックします。

1 Welcome 2 Workload Platform ... Configuration ... Summary

Welcome

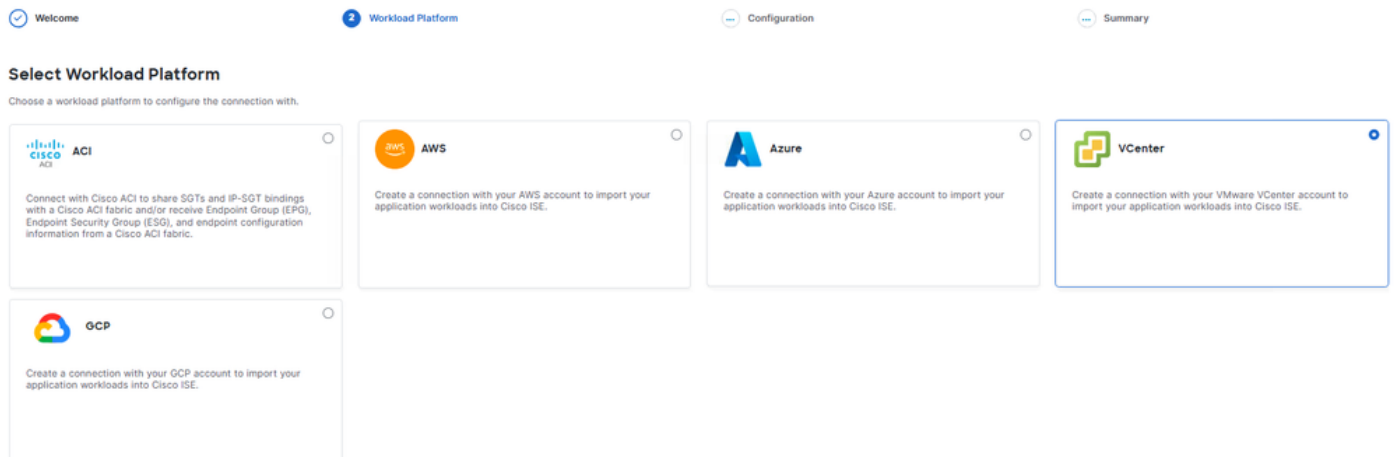
Use this wizard to set up a connection with a workload platform, and choose the attributes that you want to import into Cisco ISE
After the completion of this workflow, you can create workload classification rules, create ingress filters, and more, in Cisco ISE TrustSec pages.



ワークロード接続ウィザードの「ようこそ」ページ。ウィザードの「ようこそ」、「ワークロード・プラットフォーム」、「構成

」、および「要約」の各段階が表示されます。

4. Select Workload PlatformページでvCenterを選択し、Nextをクリックします。



ACI、AWS、Azure、およびGCPプラットフォームの中からvCenterオプションを選択してワークロードプラットフォームページを選択します

5. ワークロード接続の作成ページでは、Cisco ISEが接続の詳細を受け入れる前に、ワークロードコネクタサービスが実行されているかどうかを確認します。

サービスがまだ実行されていない場合は、ページに「Workload Connector Services are not running」と表示されます。

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. ⓘ

ワークロードコネクタサービスが実行されていないことを報告するワークロード接続ページを作成します

Cisco ISEはサービスを自動的に開始し、進行状況を表示します。

Create Workload Connection

Checking Prerequisites

Starting the services

80%

Workload Connection Name*

Non-editable after creation

Description

Sync Interval*

15

Minutes

▼

FQDN or IP address*

Hint

User*

Password*

☐ Validate vCenter certificate. ⓘ

ワークロード・コネクタ・サービスの開始を示す「ワークロード接続の作成」ページ

ページに「Workload Connector Services are running」と表示されるまで待ちます。接続の詳細フィールドは、このチェックが成功した後にのみ入力できます。

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. ⓘ

ワークロード・コネクタ・サービスが実行されていることを確認する「ワークロード接続の作成」ページ

6. 接続の詳細を入力します。

フィールド	説明
ワークロード接続名	文字、数字、およびアンダースコアを使用する一意の名前。最大32文字で、スペースは使用できません。この例では、LAB_VCenterを使用します。
説明	接続の説明。
同期間隔	Cisco ISEがvCenterからのデータを更新する頻度有効な範囲は60秒～7日です。デフォルトは 15 分です。間隔が短いほどデータの更新頻度は高くなりますが、パフォーマンスに影響を与える可能性があります。
FQDNまたはIPアドレス	vCenterのホスト名またはIPアドレス ([VCENTER_FQDN]または [VCENTER_IP_ADDRESS]など)。この値は、vCenterエンドポイント証明書のサブジェクト代替名(SAN)と一致する必要があります。

フィールド	説明
User	vCenterアカウントのユーザ名、[USERNAME]
[パスワード (Password)]	vCenterアカウントパスワード[PASSWORD]。
vCenter証明書の 検証	オプション。証明書を検証し、vCenterルート証明書をCisco ISE信頼できる証明書ストアにインポートします。インポート中に、Trust for authentication of Cisco Servicesにもチェックマークを付けます。証明書の検証は、実稼働環境に推奨されます。

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. ⓘ

完了したvCenter接続の詳細フィールドと[vCenter証明書の検証]チェックボックスが選択された状態で[ワークロード接続の作成]ページ

この図では、Userフィールドにプレースホルダが表示されています。環境に適用するクレデンシャルを入力します。



注: Cisco ISEは、入力された情報を検証します。いずれかの詳細が正しくない場合、Cisco ISEはエラー「Test connection failed」。

7. [Next] をクリックします。Cisco ISEが接続をテストし、「Test connection is successful」メッセージで結果を確認します。



vCenterへのテスト接続が成功したことを確認する成功の通知

vCenterへのテスト接続が成功したことを確認する成功の通知

8. Manage Attributesページで、Cisco ISEディクショナリに追加するvCenter属性を選択します。この例では、os属性が含まれていることを確認してください。次に [Next] をクリックします。

- 学習したすべての属性を一度に含めるには、ディクショナリ内のすべてを含めるトグルを有効にします。
- 属性の名前を変更するには、Attribute Name in Dictionaryフィールドを編集します。
- 続行するには、少なくとも1つの属性を追加する必要があります。
- ^、=、"、\、|、:、[、または]などの特殊文字を含む属性名は無効であり、追加できません。

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	--

[ディクショナリにすべて含める]切り替えが有効で、学習されたvCenter属性が一覧表示された状態での[属性を管理]ページ

リストをスクロールして、接続がvCenterから学習したすべての属性 (vmid、uuid、os、network、macAddress、VM-Name、host、Power、guest.guestFullNameなど) を確認します。

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 >

[属性を管理]ページがスクロールされ、学習されたvCenter属性とレコード数の完全なリストが表示されます

9. Summaryページで、設定を確認します。値を変更するには、任意のセクションの横にあるEditをクリックします。

✓ 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

Back

Create

選択したV-CENTERワークロードプラットフォームとディクショナリに含まれる属性を示す要約ページ

10. [Create] をクリックします。Cisco ISEは、「Connection successfully created」メッセージで結果を確認します。



ワークロード接続が作成されたことを確認する成功通知

新しいvCenterコネクタが[ワークロード接続]ページに表示されます。Cisco ISEがvCenterとのセッションを確立している間、ステータスはConnectingです。

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)						

接続状態の新しいvCenterコネクタが表示された[ワークロードの接続]ページ

ステップ 2 ディクショナリへのvCenter属性の追加 (オプション)

カスタム属性を追加する場合のみ、この手順を実行します。Manage Attributesステップで選択した属性がvCenterディクショナリに自動的に追加されるため、ここで何も操作しなくても統合は機能します。辞書属性は、接続が作成された後にいつでも管理できます。

1. Work Centers > TrustSec > Integrations > Workload Connectorsの順に選択します。
2. Attributes Dictionaryをクリックします。
3. Add Attributeをクリックします。
4. Include in Dictionaryトグルを有効にします。
5. Workload Attributeフィールドに、osなどの属性名を入力します。
6. Attribute Name in Dictionaryフィールドに、表示する名前を入力します。
7. [Save] をクリックします。

次のディクショナリの動作に注意してください。

- 接続タイプごとに1つのディクショナリが作成されます。すべてのvCenterコネクタは、1つのvCenterディクショナリを共有します。
- 接続が削除されても、属性は自動的に削除されません。使用されていない属性は、手動で削除できます。
- 属性はプロバイダからインポートでき、プロバイダに存在しない属性は手動で追加できます。

ステップ 3 ワークロードをSGTに分類

ワークロード分類ルールは、インポートされたvCenterタグを含むワークロード属性を評価し、SGTを割り当てます。このステップにより、統合のセグメンテーションの価値が得られます。

SGT割り当ては、次の項目で説明されているように動作します。

- プライマリSGTはpxGridセッショントピックでセキュリティグループとしてマークされ、SXPを介したIPからSGTへのマッピングの公開に使用されます。
- セカンダリSGTは、セカンダリセキュリティグループという名前の順序付き配列としてpxGridセッショントピックに含まれています。
- 複数のルールが一致し、複数のプライマリSGTが割り当てられている場合、最初に割り当てられたSGTだけがプライマリとして扱われます。残りのSGTはセカンダリになります。

この例の分類ルールを作成するには、次の手順を実行します。

1. Work Centers > TrustSec > Integrations > Workload Classificationの順に選択します。
2. Add Classification Ruleをクリックします。
3. RULE SETTINGS領域で、Rule Nameを入力し、StatusをEnabledに設定します。
4. AUTHORIZATION CONFIGURATION領域で、Primary SGTドロップダウンリストから、[SGT_NAME]など、ルールによって割り当てられるSGTを選択します。この例では、Production_Servers SGTを割り当てます。
5. 必要に応じて、「セカンダリSGT (オプション)」ドロップダウンリストから1つ以上のセカンダリSGTを選択します。
6. RULE CONFIGURATION領域で、照合条件を作成します。属性ドロップダウンリストから、インポートしたvCenter属性 (Vcenter - osなど) を選択し、Equals演算子を選択して、一致させる値を入力します。この例では、CentOS 4/5 (64ビット) と一致します。
7. さらにルールを絞り込むには、Add Conditionをクリックして、条件をANDまたはORと組み合わせます。この例では、IP Equals演算子を使用してルールを単一ホストアドレス 192.168.10.33/32に制限するIP Address条件を追加します。
8. オプションで、Previewをクリックして、SGTの詳細とルールに一致するワークロードを確認します。
9. [Add] をクリックします。



注意: Equals演算子には完全な属性値が必要です。vCenterでは、ゲストオペレーティン

グシステムはCentOSなどの短い名前としてではなく、CentOS 4/5 (64ビット) などの完全な説明文字列としてレポートされます。その値に対してEquals CentOSをテストするルールは一致せず、暗黙のうちに失敗します。コネクタはワークロードをインポートし続けますが、SGTは割り当てられません。「検証」セクションの説明に従って、ルールを構築する前にコンテキストの可視性で正確な値を確認するか、ゲストオペレーティングシステムファミリと照合する場合は「含む」などの演算子を使用します。

Add Classification Rule

RULE SETTINGS

Rule Name*

VM

Status

☒ Enabled ☐ Disabled

AUTHORIZATION CONFIGURATION

Primary SGT *

Production_Servers

Secondary SGTs (Optional)

RULE CONFIGURATION ⓘ

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

vCenter os属性がCentOS 4/5 (64ビット) で、IPアドレスが192.168.10.33/32の場合に、Production_ServersプライマリSGTを割り当てる分類ルールページを追加します。

分類するワークロードの追加グループごとに、これらの手順を繰り返し、各ルールに異なるプライマリSGTを割り当てます。

次のルールの動作に注意してください。

- ・ルールは、ドラッグアンドドロップで並べ替えることができます。優先順位は順序によって決まります。
- ・新しい規則または重複する規則は、既存の規則の前または後に挿入できます。
- ・デフォルトの分類ルールは常にリストの一番下にあり、デフォルトでは無効になっており、UnknownプライマリSGTにマッピングされています。

- ・ 保存する前にSGTの詳細と一致するルールを確認するには、プレビューオプションを使用します。

ステップ 4着信および発信SGTドメイン規則によるルートバインディング

SGTドメインは、ネットワークのどの部分が特定のSGTバインディングを受信するかを制御します。受信規則が定義されていない場合、ワークロードコネクタから受信したバインディングはデフォルトのSGTドメインに送信されます。

インバウンドSGTドメインルールを追加します。

1. Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rulesの順に選択します。
2. Inbound SGT Domain Rulesタブで、Add Inbound Ruleをクリックします。
3. Rule Settings領域で、ルール名を入力します。
4. [Enabled] をクリックします。
5. Destinationドロップダウンリストから、バインディングを受信する必要があるSGTドメインを選択します。ドメインを追加するには、Create SGT Domainを使用します。
6. Rule Configuration領域で、SGT Name、Source、IP Addressなどの属性、またはosなどのディクショナリに追加されたvCenter属性から条件を作成します。必要に応じて、条件をANDおよびORで結合します。
7. Addをクリックし、次にSaveをクリックする。

アウトバウンドSGTドメインルールを追加します。

1. 同じページでOutbound SGT Domain Rulesタブを開き、Add Outbound Ruleをクリックします。
2. ルール名を入力して、Enabledをクリックします。
3. Destinationドロップダウンリストから、SGTの送信先を選択します。
4. Rule Configuration領域で、SGT Domains、SGT Name、またはIP Addressから条件を作成します。
5. 必要に応じて、「契約の構成」領域で、共有セキュリティグループに対して「消込済」契約と「提供済」契約を割り当てます。
6. Addをクリックし、次にSaveをクリックする。

着信および発信ルールの追加または編集時にPreviewオプションを使用して、一致するIP-SGTバインディングを確認します。

確認

このセクションでは、設定が正常に動作していることを確認します。

接続ステータスの確認

Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connectionsの順に選択し、vCenter接続がConnectedステータスで表示されていることを確認します。このページから、接続の再接続、中断、または削除を行うこともできます。

Workload Connections

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

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

Connectedステータス、受信したSGTバインディングスカウンタ、同期間隔、および最終更新時刻を示すvCenterコネクタを表示するワークロード接続ページ

分類ルールがワークロードと一致する前にキャプチャが取得されたため、この図の「Received SGT Bindings」列が0になっています。Connectedステータスがバインディングカウンタ0とともに表示されている場合は、Cisco ISEがvCenterに正常に到達したものの、まだSGTが何にも割り当てられていないことを意味します。ルールが一致すると、Cisco ISEによって生成されたバインディングの数がこのカラムに表示されます。

セキュリティグループの確認

Work Centers > TrustSec > Components > Security Groupsの順に選択し、予期されるSGTが存在することを確認します。この例では、Production_Servers SGTが存在することを確認します。

IP-SGTバインディングの確認

Work Centers > TrustSec > SXP > SGT Bindingsの順に選択し、正しい送信元と適用された分類ルールを使用してワークロードIPアドレスが正しいSGTにバインドされていることを確認します。

ワークロードのライブセッションの確認

Operations > Workloads > Live Sessionの順に選択すると、Workload Live Sessionsページが開きます。ライブセッションは、プライマリポリシー管理ノード(PAN)でのみ表示できます。このページでは、コネクタの種類によるセッションのフィルタリング、列の表示、非表示、並べ替え、結果の並べ替え、フィルタの保存、およびCSVまたはPDF形式でのデータのエクスポートを行うことができます。

Workload Live Sessions

Filter 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

学習したワークロードごとに1行を表示したワークロードライブセッションの表。開始済みタイムスタンプ、SGTバインディングのIPアドレス、空のSGT名、セカンダリSGTと宛先の列、ソース接続名LAB_VCenter、およびデフォルトのフィルタとデフォルトの値を読み取るインバウンドSGTドメインルールとSGTドメインリンクが含まれています。



注：このキャプチャは、この例のデータを保持するカラムにトリミングされます。Outbound SGT Domain Rules列とWorkload Classification Rules列は、可視領域の右側に続き、行ごとに空になっています。また、その外側のACI固有の列も同様です。このページは、コネクタの設定ページよりも後のラボセッションでキャプチャされたため、開始タイムスタンプが、前述のワークロード接続ページに表示された最終更新時刻と一致し

ません。

各行は、Cisco ISEがコネクタから学習した1つのワークロードを表します。統合を確認するには、次の列を使用します。

カラム	確認する内容
開始	Cisco ISEがセッションを学習した時間。最近のタイムスタンプにより、コネクタがポーリング中であることが確認されます。
SGTバインディング	Cisco ISEがvCenterから受信したワークロードIPアドレス。
出典	セッションを報告したワークロード接続。データの送信元のコネクタを確認します。
インバウンドSGTドメインのルールとSGTドメイン	セッションに適用されたドメインルールとSGTドメイン。一致したルールを表示するリンクを選択します。
SGT名、セカンダリSGT、およびワークロード分類ルール	ワークロードに割り当てられたSGTと、それらを割り当てたルール。分類ルールに一致しないワークロードの場合、これらの列は空のままです。

トリミング領域の右側にあるページの右上隅のRefresh、Show、およびWithinコントロールを使用して、更新間隔、レコード数、およびタイムウィンドウを設定します。

この図では、分類ルールが一致する前にキャプチャが取得されているため、すべての行のSGT NameとSecondary SGTが空の場合は、SGT Bindings列が完全に入力されています。切り抜き領域の外側にあるワークロード分類ルール列も同じ理由で空です。この組み合わせはそれ自体で有用な診断です。コネクタがvCenterからワークロードを正しく取得しており、問題が接続ではなくルール条件にあることを確認します。これが表示されたら、ステップ3に戻り、そのステップの「注意」で説明されているように、Context Visibilityによってレポートされる属性値と照合値を確認します。

コンテキストの可視性でのワークロードの可視性の確認

 バージョン要件:ワークロードコネクタエンドポイントダッシュボードは、Cisco ISE 3.5 Patch 3以降で使用できます。Cisco ISE 3.4では、前のセクションで説明したワークロードライブセッションページを使用します。

Cisco ISEは、Context Visibility内に専用のワークロードコネクタエンドポイントダッシュボードを提供します。ワークロードコネクタから収集されたエンドポイント属性データを、フィルタリング可能な1つのビューで収集、分析、レポートします。

ビューを開くには、次の手順に従います。

1. Cisco ISE GUIで、Context Visibility > Endpointsの順に選択します。
2. Workload Connector Endpointsタブを開きます。タブストリップにタブが表示されていない場合は、Moreをクリックします。
3. Connectorドロップダウンリストから、エンドポイントを確認するワークロード接続を選択します。

このウィンドウには、ワークロードコネクタからフェッチされたエンドポイント属性データが表示されます。各行は、IP Address、sourceType、およびConnector Nameによってエンドポイントを識別します。

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 here 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

[Context Visibility]の下で[Workload Connector Endpoints]ビューには、vCenterワークロードエンドポイントがIPアドレス、ソースタイプ、コネクタ名で表示され、[Connector]ドロップダウンリストはLAB_VCenterに設定され、[Export]オプション、[Rows/Page]および[pagination]コントロール、および合計行数は23行に設定されています

このビューでは、次の操作を実行できます。

- リストをフィルタリングします。列ヘッダーの下でフィルタ行を使用して、IPアドレス、送信元タイプ、またはコネクタ名によって結果を絞り込みます。フィルタは加算的であるため、適用する値ごとに結果セットが絞り込まれます。

- 結果を順に表示します。ページサイズの変更とページ間の移動には、行/ページコントロールとページ移動矢印を使用します。エンドポイントの合計数は、矢印の右側に23 Total Rowsとして表示されます。
- データをエクスポートします。Exportをクリックして、表示されたエンドポイントデータをダウンロードします。
- エンドポイントを検査します。エンドポイントのIPアドレスをクリックして、詳細スライドインペインを開きます。

詳細ペインには、選択したエンドポイントに対してCisco ISEが保持するすべての属性が表示されます。Downloadをクリックして属性の詳細を保存するか、Cancelをクリックしてペインを閉じます。

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

選択したワークロードエンドポイントの詳細スライドインペイン。コネクタ名とエンドポイントアドレスの上に詳細というタイトルが付けられ、その仮想マシン用にCisco ISEが収集したvCenterプロパティのATTRIBUTESリスト、およびキャンセルとダウンロードのコントロールが表示されます。

このペインは、ワークロード接続名とエンドポイントアドレスで識別されます (LAB_VCenter_192.168.10.1として表示されます)。vCenterワークロードエンドポイントの属性には、vCenterから学習した仮想マシンプロパティ (Power、VM-Name、host、macAddress、network、os、uuid、vmid、vmtypeなど) と、コネクタメタデータcorrelationId、source、ipAddress、connectorType、およびSourceTypeが含まれます。ディクショナリに追加したカスタムvCenterタグもここに表示されます。

このペインは、分類規則が一致する必要がある値の正規のソースです。最初にチェックすると、このワークフローで最も一般的なエラーを回避できます。この図では、osはCentOS 4/5 (64ビット) を読み取ります。これは、Equals条件で再現する必要がある完全な文字列です。CentOSなどの短い形式を使用する代わりに、ステップ3でルールを記述する前に、この値を読んでください。



注：エンドポイントごとに最大50個の属性が表示されます。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

一般的な問題

症状	考えられる原因	アクション
コネクタのセットアップ中にテスト接続に失敗しました	1つ以上の接続の詳細が正しくないか、前提条件を満たしていません	FQDNまたはIPアドレスを確認し、証明書SANに一致することを確認します。ユーザ名とパスワードを確認し、証明書の検証設定を確認し、プロキシバイパスと時刻同期の前提条件が満たされていることを確認します。

症状	考えられる原因	アクション
コネクタは作成されていますが、データはインポートされていません	Cisco ISEがpublic.ecr.awsにアクセスできない	プロキシまたはファイアウォールがこのURLへのTCPポート443のHTTPSトラフィックを許可していることを確認します。
ワークロードはインポートされるがSGTは割り当てられず、受信SGTバインディングは0のままである。	分類ルールが実際の属性値と一致しません。最も一般的な原因は、CentOS 4/5 (64ビット) ではなくCentOSなどの部分値に対してテストされたEquals条件です	Context VisibilityでDetailsペインを開き、正確な属性値を読み取ってルール条件を修正するか、演算子をContainsに変更します。この障害はサイレントです。コネクタ自体が正常なため、アラームは発生しません。
接続がSuspended状態に移行する	接続に関連付けられたすべてのSGTが削除されました	必要なSGTを再作成し、接続を再確立します。関連するSXPバインディングおよびMnTセッションデータは、接続が中断している間は削除されます。
PSNの再起動後に接続の詳細が失われる	セッションデータは再入力されませんでした	接続を中断し、再接続します。

デバッグログの有効化

PAN、SXP、およびpxGridノード上で、Operations > Troubleshoot > Debug Wizard > Debug Profile Configurationの順に選択し、Workload Connectorコンポーネントのデバッグログ重大度をDEBUGに設定します。

これらのログファイルは/opt/CSCOCpm/logsにあります。

ログファイル	コンテンツ
ワークロード.log	ワークロードコネクタの動作。
workload-conn/*.log (デフォルト)	接続ごとのログ。
apiサービス.log	APIサービスのアクティビティ。
ise-psc.log	Cisco ISEポリシーサービスアクティビティ。

ログファイル	コンテンツ
pxgriddirect-service.log (ストリーミングエラー)	pxGrid Directサービスのアクティビティ。
sxp_appserver/sxp.log	SXPバインディングの配布。

アラーム

Cisco ISEは、vCenterおよびその他のクラウドコネクタに対して次のアラームを生成します。

アラーム	次の場合に発生
ワークロード接続の作成/接続に失敗しました	復元、プロモーション、HAイベント、またはアップグレードなどのイベントの後、コネクタの作成が失敗する。
ワークロード接続の削除に失敗しました	コネクタの削除に失敗しました。
ワークロード接続サービスエラー	関連する別のサービス障害が発生する。

関連情報

- [Cisco ISE共通ポリシーおよびワークロードコネクタ](#)
- [Cisco ISEで必要なインターネットURL](#)
- [Cisco ISE 3.5管理者ガイド](#)
- [シスコテクニカルサポートおよびダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。