

Revised: July 21, 2025

Common Policy: Workload Connectors

Workload connectors

Common Policy is a framework for building and enforcing consistent access and segmentation policies, regardless of the domain. Workload connectors are used in this framework to build secure connections with on-premises and cloud data centers, import application workload context, normalize that context into SGTs, and share the context with other domains for building policies.

You can establish logical clusters of SXP devices, referred to as SGT domains, to regulate traffic according to SGT bindings. It helps you set up authorization policies and workload classification rules. With these rules, you can assign SGTs to IP addresses and receive mappings. Additionally, you can specify the SGT domains that will receive the mappings by managing incoming SGT domain rules.

Workload Classification Rules are used to assign primary and secondary SGTs to workloads. Secondary SGTs could be tagged along with Primary SGTs. Inbound SGT domain rules are used to map incoming SGT bindings to specific SGT domains. Outbound SGT domain rules are used to designate target destinations for specific SGT bindings.


For information on TrustSec, see [Cisco TrustSec](#).

Add a workload connection

Follow these steps to add a workload connection.

Before adding any workload connection:

- pxGrid must be enabled on at least one node within your network.
- SXP must be enabled on at least one node within your network.
- Identify the relevant attributes (tags) within your vCenter, AWS, GCP, or Azure environment that need to be added to workload connector.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.


Step 4 In the **Select Workload Platform** page, click the links below for directions on adding the specific workload connector platform.

- [ACI](#)
- [AWS](#)
- [Azure](#)
- [vCenter](#)
- [GCP](#)

Add a Cisco ACI connection

- Enable the pxGrid and SXP services in **Administration > System > Deployment**.

- Update the DNS configuration in Cisco ACI so that Cisco ACI can resolve the FQDN of the Cisco ISE pxGrid node.
- You will need an Advantage, Premier, or 90-day evaluation license for this integration.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.

Step 4 In the **Select Workload Platform** page, click **ACI**.

Step 5 In the **Create ACI Connection** page, enter the following details:

- **ACI Connection Name:** Enter a name for the connection.
- **FQDN or IP Address:** Enter the IP address or FQDN of the Cisco ACI server.
- **ACI Username:** Enter the username of the Cisco ACI admin user.
- **ACI Password:** Enter the password of the Cisco ACI admin user.
- **Login Domain (Optional):** Enter an authentication domain for the Cisco ACI connection.
- **Validate ACI Certificate:** If you enable this option, Cisco ISE will need the ACI controller's certificate in its Trusted Certificate store. When this option is disabled, Cisco ISE will not validate the ACI certificates. We recommend that you enable this option in the production environment. For information on how to import certificates into the Cisco ISE Trusted Certificate Store, see [Import a Root Certificate into the Trusted Certificate Store](#).

Upon connecting to this controller, Cisco ISE automatically retrieves the FQDNs and IP addresses of other controllers connected to the same Cisco Application Policy Infrastructure Controller (APIC) site.

When the connection is verified, click **Next**.

Step 6 In the **Naming Convention** page, set the naming convention for the SGTs that will be created from the EPGs and ESGs received from the connected Cisco ACI controllers.

You can use the following types of naming conventions to create SGT names with up to 64 characters:

- **Use ACI Attribute Values:** Choose the EPG or ESG attributes whose values must be combined to form the name of the newly created SGTs. These attributes will be added to the name suffix of the newly created SGTs. You can choose any of the following attributes:

- **Connection Name**
- **Tenant**
- **VRF**
- **Application Profile**
- **Endpoint Group Type**

You can use the default attribute values or create custom values.

- **Append Prefix or Suffix:** Enter a prefix or suffix that will be added to the existing name of the EPG or ESG.

**Note**

- If you are using a Cisco Catalyst Center version earlier than 2.3.7.7, the maximum character limit for SGT names is 32.
- If any of your integrated applications do not support more than 32 characters, you must consider this limitation while configuring the naming conventions for SGT names in Cisco ISE.

Step 7 Click **Next**.

Step 8 In the **Select EPG/ESGs** page, select the EPGs or ESGs that must be retrieved from Cisco ACI and converted to SGTs.

You will be able to use the **Select All** option during the initial setup. After configuring the SGT numbering range, you cannot choose the **Select All** option if the number of listed EPG or ESGs is greater than the numbering range configured.

If a security group name populated from the connection already exists in the Cisco ISE database, the SGT isn't assigned a new number. If the security group name does not exist in the Cisco ISE database, then a new security group will be created with the derived name and an SGT will be assigned from the available SGT range.

While editing this connection, you cannot deselect an EPG that is used in an inbound or outbound SGT domain rule.

Step 9 Click **Next**.

Step 10 (Optional) In the **Set SGT Numbering Range** page, enable the **Set SGT Numbering Range for EPG/ESGs** option to manually configure a numbering range for the newly created SGTs.

While setting the numbering range, account for existing and expected EPGs and ESGs.

When this option is disabled, Cisco ISE automatically assigns numbers to SGTs from the number ranges that are not reserved or used for other SGTs.

Step 11 Click **Next**.

Step 12 Verify the entered details in the **Summary** page. You can click **Edit** in the corresponding section to update the details, if needed.

Step 13 Click **Create**.

To verify whether the Cisco ACI connection is successfully created:

- Verify the connection status in the **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections** page.
- Check whether the EPGs and ESGs that are selected in Step 7 are converted to security groups in the **Work Centers > TrustSec > Components > Security Groups** page.
- Verify whether the bindings for the EPGs and ESGs that are selected in Step 7 are listed in the **Work Centers > TrustSec > SXP > SGT Bindings** page.

You can connect, suspend, or delete a connection from the **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections** page.

If all the associated SGTs are deleted for a connection, the connection will be moved to **Suspended** state. When a connection is in **Suspended** state:

- All SXP bindings and MnT session data related to that connection are removed.
- ACI connection subscription is paused.




Note

- Modifications to the name conversion rule will not be automatically applied to the EPGs or ESGs already learned from this Cisco ACI connection. To apply the modified name conversion rule, you must first deselect the previously learned EPGs or ESGs from the **Synced EPG/ESGs** tab and save your changes. After that, you must edit the connection again to select the required EPGs or ESGs, and then save your changes again.
- If the PSNs are restarted, you must suspend and reconnect the ACI connection to repopulate the ACI connection details.
- If you are using multiple ACI connections, you must configure the SXP nodes identically to listen to same NADs.

Add an AWS workload connector

Make sure to fulfill these prerequisites before adding an AWS workload connector:

- You must have a stable internet connection.
- You must have a policy that grants these permissions: **ec2:DescribeTags**, **ec2:DescribeVpcs**, and **ec2:DescribeInstances**.
- You must ensure Cisco ISE server time is synchronized correctly, with a time delta of no more than 5 minutes.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.

Step 4 In the **Select Workload Platform** page, choose **AWS**.

Step 5 Enter these details while adding the AWS connection.

- **Workload Connection Name:** Enter a unique connection name. The connection name can include letters, numbers, and underscores. It must have only 32 characters and no spaces.
- **Description:** Enter the description of the connection.
- **Sync Interval:** Enter a value ranging from 60 seconds to 7 days, using seconds, minutes, hours, or days as units. By default, the sync interval is set to 15 minutes. You can adjust the sync interval based on how often you want the data to be refreshed. However, setting a shorter interval could potentially lead to performance issues.
- **Region:** Enter the region where the AWS workload is configured.



You can create multiple AWS workload connectors to support various regions.

Note

- **AWS Access Key:** Enter the private AWS access key.
- **AWS Secret Key:** Enter the private AWS secret key.

Step 6 Click **Next**.

Step 7 In the **Manage Attributes** page, choose the existing AWS attributes (tags) that you want to add to the Cisco ISE dictionary, and then click **Next**.

You can rename the attribute in the **Attribute Name in Dictionary** field.

**Note**

- You must add at least one attribute to the dictionary to proceed to the next step.
- Attributes with special characters like ^, =, ", ` , |, :, and [] are invalid and cannot be added to the dictionary.

Step 8 In the **Summary** page, review the Cisco ISE workload connector configurations. Click **Edit** to change any configuration.


Step 9 Click **Create**.

The newly created AWS connectors are listed in the **Workload Connections** listing page.

Add an Azure workload connector

Make sure to fulfill these prerequisites before adding an Azure workload connector:

- You must have a stable internet connection.
- You must have a policy with **Reader** permission.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.

Step 4 In the **Select Workload Platform** page, choose **Azure**.

Step 5 Enter these details while adding the Azure connection.

- **Workload Connection Name:** Enter a unique connection name. The connection name can include letters, numbers, and underscores. It must have only 32 characters and no spaces.
- **Description:** Provide additional information about the workload connector (maximum of 2000 characters).
- **Sync Interval:** Enter a value ranging from 60 seconds to 7 days, using seconds, minutes, hours, or days as units. By default, the sync interval is set to 15 minutes. You can adjust the sync interval based on how often you want the data to be refreshed. However, setting a shorter interval could potentially lead to performance issues.
- **Subscription ID:** Enter the 32-digit subscription ID of the Azure account. You can locate this information from **Home > Subscriptions**.
- **Tenant ID:** Enter the Tenant ID. You can locate this information in your Azure web portal. Log in to your account, select your **Microsoft Entra ID**, and then navigate to the **Basic Information** section under **Overview** tab.
- **Client ID:** Enter the client ID. You can locate this information by logging into the Azure portal and then selecting **App registrations** under **Entra ID**. Choose the Azure AD app you want to find the Client ID for and then click the app to open its details. The client ID is listed under **Essentials**.
- **Client Secret:** Enter the private client secret key.

**Note**

Cisco ISE validates the added information for each of the connection types and returns the error "**Test connection failed**" if any of the details are incorrect.

Click **Next**.

Step 6 In the **Manage Attributes** page, choose the existing Azure attributes (tags) that you want to add to the Cisco ISE dictionary, and then click **Next**.

You can rename the attribute in the **Attribute Name in Dictionary** field.



Note

- You must add at least one attribute to the dictionary to proceed to the next step.
- Attributes with special characters like ^, =, ", ` , |, :, and [] are invalid and cannot be added to the dictionary.

Step 7 In the **Summary** page, review the Cisco ISE workload connector configurations. Click **Edit** to change any configuration.

Step 8 Click **Create**.

The newly created Azure connectors are listed in the **Workload Connections** listing page.

Add a vCenter workload connector


Make sure to fulfill these prerequisites before adding a vCenter workload connector:

- You must have a stable internet connection.
- You must have a policy with **Read Only** permission.
- If a proxy is needed to access the internet, you must bypass the vCenter IP if the vCenter is on-premises.



Note

As VMware ESXi does not support attributes (tags), only vCenter can be configured as a workload connector.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.

Step 4 In the **Select Workload Platform** page, choose **vCenter**.

Step 5 Enter these details while adding the vCenter connection.

- **Workload Connection Name:** Enter a unique connection name. The connection name can include letters, numbers, and underscores. It must have only 32 characters and no spaces.
- **Description:** Enter the description of the connection.
- **Sync Interval:** Enter a value ranging from 60 seconds to 7 days, using seconds, minutes, hours, or days as units. By default, the sync interval is set to 15 minutes. You can adjust the sync interval based on how often you want the data to be refreshed. However, setting a shorter interval could potentially lead to performance issues.
- **FQDN or IP Address:** Enter the hostname or IP address. The value entered here should match the **Subject Alternative Name** of vCenter's endpoint certificate.
- **User:** Enter the username of your vCenter account.
- **Password:** Enter the password of your vCenter account.
- **Validate vCenter certificate:** (Optional) Check the check box to validate the certificate and import vCenter's root certificate to ISE's **Trusted Certificates** store. You must check the **Trust for authentication of Cisco Services** check box when importing the certificate.

**Note**

Cisco ISE validates the added information for each of the connection types and returns the error "**Test connection failed**" if any of the details are incorrect.

Step 6 Click **Next**.

Step 7 In the **Manage Attributes** page, choose the existing vCenter attributes (tags) that you want to add to the Cisco ISE dictionary, and then click **Next**.

You can rename the attribute in the **Attribute Name in Dictionary** field.

**Note**

- You must add at least one attribute to the dictionary to proceed to the next step.
- Attributes with special characters like ^, =, ", ` , |, :, and [] are invalid and cannot be added to the dictionary.

Step 8 In the **Summary** page, review the Cisco ISE workload connector configurations. Click **Edit** to change any configuration.


Step 9 Click **Create**.

The newly created vCenter connectors are listed in the **Workload Connections** listing page.

Add a GCP workload connector

Make sure to fulfill these prerequisites before adding a GCP workload connector:

- You must have a stable internet connection.
- You must have a policy with **Basic > Viewer** permission.

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors > Workload Connections**.

Step 2 Click **Add Connection**.

Step 3 Click **Let's do it**.

Step 4 In the **Select Workload Platform** page, choose **GCP**.

Step 5 Enter these details while adding the connection, and then click **Next**.

- **Workload Connection Name:** Enter a unique connection name. The connection name can include letters, numbers, and underscores. It must have only 32 characters and no spaces.
- **Description:** Enter the description of the connection.
- **Sync Interval:** Enter a value ranging from 60 seconds to 7 days, using seconds, minutes, hours, or days as units. By default, the sync interval is set to 15 minutes. You can adjust the sync interval based on how often you want the data to be refreshed. However, setting a shorter interval could potentially lead to performance issues.
- **GCP Region:** Enter the region where the GCP workload is configured, for example, us-east1.

**Note**

You can create multiple GCP workload connectors to support various regions.

- **Service Account:** Enter the service account information by either copying and pasting the file text or clicking **Import Service Account** and uploading the file.

**Note**

Cisco ISE validates the added information for each of the connection types and returns the error "**Test connection failed**" if any of the details are incorrect.

Step 6 In the **Manage Attributes** page, choose the existing GCP attributes (tags) that you want to add to the Cisco ISE dictionary, and then click **Next**.

You can rename the attribute in the **Attribute Name in Dictionary** field.

**Note**

- You must add at least one attribute to the dictionary to proceed to the next step.
- Attributes with special characters like ^, =, ", ` , |, :, and [] are invalid and cannot be added to the dictionary.

Step 7 In the **Summary** page, review the Cisco ISE workload connector configurations.

Step 8 Click **Edit** to change any configuration.

Step 9 Click **Create**.

The newly created GCP connectors are listed in the **Workload Connections** listing page.


Attributes dictionary

Attributes dictionary lists the attributes for all the workload connections (except ACI) integrated with Cisco ISE. You can select and add the required attributes to the Cisco ISE dictionary.

Note the following points while configuring the attributes.

- One dictionary will be created for each connection type. For example, attributes of all AWS connectors will be added to a single AWS dictionary.
- Attributes in use will not be excluded from the dictionary.
- Attributes will not be automatically removed when you delete a connection.
- You can manually delete any attribute that is not in use.
- You can import new attributes from provider.
- You can add attributes that are not present in the provider.

Add dictionary attributes

Step 1 In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Connectors**.

Step 2 Click **Attributes Dictionary**.

Step 3 Click **Add Attribute**.

Step 4 Enable the **Include in Dictionary** toggle button.


Step 5 Enter the attribute name in the **Workload Attribute** field.

Step 6 Enter the name to be displayed in the dictionary in the **Attribute Name in Dictionary** field.

Step 7 Click **Save**.

Add inbound SGT domain rules

You can create inbound SGT domain rules to map incoming SGT bindings with specific SGT domains. If no rules are defined, bindings received from workload connectors are sent to the default SGT domain.

- Step 1** In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules**.
- Step 2** In the **Inbound SGT Domain Rules** tab, click **Add Inbound Rule**.
- Step 3** In the **Rule Settings** area, enter the name of the inbound SGT domain rule.
- Step 4** Click **Enabled**.
- Step 5** From the **Destination** drop-down list, choose the SGT domains to which the bindings must be sent.
Use the **Create SGT Domain** option to create a new SGT domain and add it to the destination list.
- Step 6** In the **Rule Configuration** area, configure the conditions for the inbound SGT domain rule using the following attributes:
- **EPG**
 - **SGT Name**
 - **Source**
 - **Tenant**
 - **VRF**
 - **IP Address**

You can also choose from the additional attributes (tags) that you added to the dictionary while creating AWS, GCP, Azure, and vCenter workload connectors.

You can also add AND or OR conditions based on your requirements.


Step 7 Click **Add**.

Step 8 Click **Save**.

You can create outbound SGT domain rules to designate target destinations for specific SGT bindings. For information on how to create outbound SGT domain rules, see [Add outbound SGT domain rules, on page 9](#).

Add outbound SGT domain rules

You can create outbound SGT domain rules to designate target destinations for specific SGT bindings.

- Step 1** In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules**.
- Step 2** In the **Outbound SGT Domain Rules** tab, click **Add Outbound Rule**.
- Step 3** In the **Rule Settings** area, enter the name of the outbound SGT domain rule.
- Step 4** Click **Enabled**.
- Step 5** From the **Destination** drop-down list, choose the Cisco ACI connections and the Layer 3 Outs (L3Outs) to which the SGTs must be sent.

- Step 6** In the **Rule Configuration** area, configure the conditions for the outbound SGT domain rule using the following attributes:
- **SGT Domains**
 - **SGT Name**
 - **IP Address**

You can also add AND or OR conditions based on your requirements.

Step 7 (Optional) In the **Contract Configuration** area, assign **Consumed** and **Provided** contracts for the shared security groups.

Step 8 Click **Add**.

Step 9 Click **Save**.

After creating the outbound SGT domain rules, you can verify the ACI consumer status in the **Administration > pxGrid Services > Diagnostics > WebSocket > Topics** page.

You can use the **Preview** option to preview the matching IP-SGT bindings while adding or editing the inbound and outbound SGT domain rules.

You can view the newly created inbound and outbound SGT domain rules in the **Work Centers > TrustSec > SXP > Inbound & Outbound SGT Domain Rules** page. To view the SGT bindings table for a specific filter, click its SGT bindings number.



When you configure an outbound SGT domain rule, you must choose an SGT that doesn't originate from the destination ACI. If you choose an SGT that originates from the destination ACI, Cisco ISE pushes the selected SGT binding back to the originating ACI.

Add workload classification rules

Workload classification rules are used to classify the workloads and to assign primary and secondary SGTs to the workloads. The primary SGT is marked as “Security Group” in the pxGrid session topic and is used to publish IP-to-SGT mappings via SXP. Secondary SGTs are included in the pxGrid session topic as an ordered array named “Secondary Security Groups.”

You can specify the order of classification rule execution. You can drag and drop the rules to change the order of priority.

You can insert a new or duplicate rule above or below an existing rule based on the priority that you want to set for that rule.


The default classification rule is always listed at the bottom of the list. The default rule is disabled by default and mapped to **Unknown** primary SGT.

If multiple classification rules are matched and multiple primary SGTs are assigned, only the first assigned SGT is considered as the primary SGT and the remaining SGTs are marked as secondary SGTs. You can create inbound SGT domain rules to define the SGT domains for these IP bindings.



For a workload from a Cisco ACI connection, the primary SGT is always the one created during connection configuration and derived from its EPG or ESG.

Follow these steps to add a workload classification rule.

- Step 1** In the Cisco ISE GUI, click the **Menu** icon () and choose **Work Centers > TrustSec > Integrations > Workload Classification**.
- Step 2** Click **Add Classification Rule**.
- Step 3** In the **Rule Settings** area, enter the name of the workload classification rule.
- Step 4** Click **Enabled**.
- Step 5** In the **Authorization Configuration** area, from the **Primary SGT** drop-down list, choose the primary SGT for that rule.
- Step 6** (Optional) From the **Secondary SGT** drop-down list, choose the secondary SGTs that you want to add to that rule.
- Step 7** In the **Rule Configuration** area, configure the conditions for the workload classification rule using the following attributes:

- **EPG**
- **SGT Name**
- **Source**
- **Tenant**
- **VRF**
- **IP Address**

You can also choose from the additional attributes (tags) that you added to the dictionary when creating AWS, GCP, Azure, and vCenter workload connectors.

You can also add AND or OR conditions based on your requirements.

- Step 8** Click **Save**.

You can use the **Preview** option to preview the SGT details and matching rules while adding or editing the workload classification rules.

The **SGT Bindings** page displays all the configured SGT bindings, giving you an easy view of assigned primary and secondary SGTs, the source of the learned data, and the workload classification rules that are applied. You can also view the IP-SGT bindings with shared destinations. You can review the classification details and the specifics of defined inbound and outbound SGT domain rules by clicking the corresponding column values.



Note

The maximum number of IP-SGT bindings supported for each network device depends on the model of device and its capacity design. For information about the Cisco SD-Access platform scale, see [Cisco Catalyst Center Data Sheet](#).

Refer to the border node scale and the edge node scale while configuring the workload classification rules for different network device types. If the total number of bindings is greater than the maximum number of bindings supported for a device, the IP-SGT bindings exceeding the scale limit are dropped and not sent to the SXP devices. In this case, you must reduce the number of IP-SGT bindings based on the scale limits and reconfigure your settings.

Troubleshoot

Workloads live session

The **Workloads Live Session** page displays the details about the live workload sessions. To view this page, in the Cisco ISE GUI, click the **Menu** icon and choose **Operations > Workloads > Workloads Live Session**.

You can view the live workload sessions only in the primary PAN.

You can do the following in the **Workloads Live Session** page:

- Filter the workload sessions based on connector type.
- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter and save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Debug logs for workload connectors

You can configure the debug log severity level for ACI in **Operations > Troubleshoot > Debug Wizard > Debug Profile Configuration**. You must set the log level as **DEBUG** for the **Workload Connector** component on the PAN, SXP, and pxGrid nodes.

The following log files are available for Workload connectors (under /opt/CSCOcpm/logs):

- workloads.log
- workload-conn/*.log
- aciconn/aciconn.log
- api-service.log
- ise-psc.log
- pxgriddirect-service.log
- sxp_appserver/sxp.log

Alarms generated for workload connectors

The following alarms are generated for the ACI integration.

- When an EPG, ESG, or L3Out is deleted in Cisco ACI, the corresponding objects are deleted in Cisco ISE. If any of those objects are included in the Inbound or Outbound rules, an alarm is raised.
- When the mdpConn object is deleted in Cisco ACI, Cisco ISE learns the configuration changes and generates an alarm.
- When an EEPG is deleted in Cisco ACI, Cisco ISE learns the configuration changes and generates an alarm.
- While deleting the ACI connection in Cisco ISE, if the process fails to delete the learned SGTs and SGT range, an alarm is generated.
- When the Cisco ISE listener listening to Cisco ACI events is disconnected from Cisco ACI, an alarm is generated. This may occur due to ACI password change, certificate expiry, or network connectivity issue.

This may also occur if the server certificate is changed in Cisco ACI during an upgrade. In this case, you must update the server certificate for Cisco ACI in the Cisco ISE Trusted Certificate Store.

These alarms are generated for vCenter and other cloud systems:

- If the creation of a workload connector fails after scenarios like restore, promotion/HA, or upgrade, **Workload Connection Create/Connect Unsuccessful** alarm is generated.
- If the deletion of a workload connector fails, **Workload Connection Delete Unsuccessful** alarm is generated.
- When other related workload connection service failures occur, **Workload Connection Service Error** alarm is generated.