Audit Logs and Security

Audit Logs

Multi-Site Orchestrator system logging is automatically enabled when you first deploy the Orchestrator cluster and captures the events and faults that occur in the environment.

You can view the Multi-Site Orchestrator logs directly in the GUI by selecting **Admin** > **Audit Logs** from the main navigation menu.

From the **Audit Logs** page, you can click the **Most Recent** field to select a specific time period for which you want to see the logs. For example, when you select the range from November 14, 2019 to November 17, 2019 and click **Apply**, the audit log details for this time period are displayed on the **Audit Logs** page.

You can also click the **Filter** icon to filter the log details using the following criteria:

- **User**: Select this option to filter the audit logs by the user type, then click **Apply** to apply the filter.
- **Type**: Select this option to filter the audit logs by the policy types, for example, site, user, template, application profile, bridge domain, EPG, external EPG, filter, VRF, BGP config, contract, OSPF policy, pod, node, port, domain, provider, RADIUS, TACACS+ and click **Apply**.
- **Action**: Select this option to filter the audit logs by an action. The available actions are Created, Updated, Deleted, Added, Removed, Associated, Disassociated, Deployed, Undeployed, Downloaded, Uploaded, Restored, Logged in, Logged Out, Login Failed. Select an action and click **Apply** to filter the log details according to the action.

Security

Cisco ACI Multi-Site Orchestrator OVA contains a self-signed SSL certificate that is stored in `/data/msc/secrets` directory on each node during the Orchestrator installation. By default, the Orchestrator GUI uses this certificate for its HTTPS connections.

While you could previously update these certificates by logging directly into an Orchestrator node server and changing its web server (`nginx`) configuration, starting with Cisco ACI Multi-Site Orchestrator Release 2.1(1), you can use the GUI to easily add or update custom certificates to be used for the Orchestrator's GUI connection.

When adding custom certificates, you can use one of the following two options:

- **Self-Signed Certificate** provide you with the ability to create your own public and private keys to be used by the Orchestrator's GUI.
- **CA-Issued Certificate** allows you to use a certificate provided by an existing Certificate Authority (CA) along with its keys.

You can add multiple CAs and Keyrings containing the public/private key combinations in the GUI, however only a single keyring can be active at any given time and used to secure the communication between the Orchestrator GUI and your browser.

Adding Custom Certificate Authority

You can add a custom Certificate Authority (CA) to be used for verifying the public key provided by the Orchestrator for HTTPS traffic encryption.

This section describes how to add and configure a custom CA in Multi-Site Orchestrator GUI. Configuring keyrings and keys is described in the next section.

Note The keyrings feature is available for ESX OVA Multi-Site Orchestrator deployments; it is not available for deployments in Application Services Engine or Nexus Dashboard.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Certificate Authority** tab and click **Add Certificate Authority**.

Step 4 In the **Add Certificate Authority** window that opens, provide the CA details.

In the **Name** field, enter the CA name.

In the **Description** field, enter the CA description.

In the **Certificate Chain** field, enter the CA's certificate chain. You must include both, intermediate and root, certificates. The intermediate certificate must be entered first, followed by the root certificate.

Step 5 Click **SAVE** to save the changes.

Adding Custom Keyring

Note This feature is available for ESX OVA Multi-Site Orchestrator deployments; it is not available for deployments in Application Services Engine or Nexus Dashboard.

You can add a custom keyring containing a public and private encryption keys to be used for Orchestrator GUI HTTPS traffic encryption.

This section describes how to add a custom keyring. For instructions on adding a Certificate Authority (CA) that can be used to verify the public key in this keyring, see the previous section.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left-hand navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Key Rings** tab and click **ADD KEY RING**.

Step 4 In the **Create Key Ring** window that opens, provide the key ring details.

From the **SELECT CERTIFICATE AUTHORITY** dropdown menu, select the certificate authority that will contain the key ring.

In the **NAME** field, enter the key ring name.

In the **KEY RING DESCRIPTION** field, enter the key ring description.

In the **PUBLIC KEY** field, enter the ring's public key.

In the **PRIVATE KEY** field, enter the ring's private key

Step 5 Click **SAVE** to save the changes.

Activating Custom Keyring

Note This feature is available for ESX OVA Multi-Site Orchestrator deployments; it is not available for deployments in Application Services Engine or Nexus Dashboard.

After you add a keyring, as described in previous section, you need to activate it as the default keyring.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 From the left-hand navigation menu, select **Admin** > **Security**.

Step 3 In the main window, select the **Key Rings** tab.

Step 4 In the main window, click the **...** icon next to the keyring you want to activate and choose **Make Keyring Active**.

Step 5 Click **ACTIVATE** to activate the keyring.

Activating a key will log you out of the Multi-Site Orchestrator GUI. When the login page is loaded, it will use the new certificate and key.

Custom Certificates Troubleshooting

The following sections describe how to resolve common issues when using custom SSL certificates with Multi-Site Orchestrator.

Unable to Load the Orchestrator GUI

If you are unable to load the Orchestrator GUI page after installing and activating a custom certificate, it is possible that the certificates were not copied correctly to each Orchestrator node. You can resolve this issue by recovering the default certificates and then repeating the new certificate installation procedure again.

To recover the default Orchestrator certificates:

1. Log in to each Orchestrator node directly.
2. Change into the certificates directory:

   ```
   # cd /data/msc/secrets
   ```

3. Replace the `msc.key` and `msc.crt` files with `msc.key_backup` and `msc.crt_backup` files respectively.

   ```
   # cp msc.key_backup msc.key
   # cp msc.crt_backup msc.crt
   ```

4. Restart the Orchestrator GUI service.

   ```
   # docker service update msc_ui --force
   ```

5. Re-install and activate the new certificates as described in previous sections.

Adding a New Orchestrator Node to the Cluster

If you add a new node to you Multi-Site Orchestrator cluster:

1. Log in to the Orchestrator GUI.
2. Re-activate the key you are using as described in previous sections.

Unable to Install a New Keyring after the default Keyring Expired

If you are unable to install a new Keyring after the default Keyring expired, it is possible that custom Keyring is not installed on the cluster nodes.

You can resolve this issue by deleting the old default Keyring and creating a new Keyring using steps mentioned below:

1. Execute the following commands on all the nodes in the cluster:

   ```
   cd /data/msc/secrets
   rm -rf /data/msc/secrets/msc.key
   rm -rf /data/msc/secrets/msc.crt
   rm -rf /data/msc/secrets/msc.key_backup
   rm -rf /data/msc/secrets/msc.crt_backup
   !
   !
   openssl req -newkey rsa:2048 -nodes -keyout /data/msc/secrets/msc.key -x509 -days 365
   -out /data/msc/secrets/msc.crt -subj '/CN=MSC'
   cp /data/msc/secrets/msc.key /data/msc/secrets/msc.key_backup
   cp /data/msc/secrets/msc.crt /data/msc/secrets/msc.crt_backup
   cd /data/msc/secrets
   chmod 777 msc.key
   ```

```
chmod 777 msc.key_backup
chmod 777 msc.crt
chmod 777 msc.crt_backup
```

2. Execute the following command to force update of **msc_ui** service:

   # docker service update msc_ui --force

3. Once the update completes, check if all the replicas of **msc_ui** are healthy.

```
[root@node1 ~]# docker service ls
...
rqs0607lgixg     msc_ui     global     3/3    msc-ui:3.1.1i
*:443->443/tcp
```

4. Log in to any of the MSO nodes using any browser. If the browser is stuck in a loop while accepting the certificate details or displays a white screen, refresh the page one or two times until the GUI is displayed normally again.
5. Log in using the username and password and activate the Keyring by following the steps described in the '*Activating Custom Keyring*' section.