Monitoring and Reporting

This chapter contains the following sections:

About Monitoring and Reporting

Cisco UCS Director displays all managed Cisco UCS components in each Cisco UCS domain that has been added as a Cisco UCS Manager account. These components can be hardware or software.

Reports

Cisco UCS Director provides several different kinds of reports that you can use to view the status of a Cisco UCS Manager pod and its components. All of these reports can be manually refreshed for real-time data and exported to PDF, CSV, or XLS format for you to share with others.

The available reports include:

- **Summary reports** for comparison data and other information about the components of the pod. These reports display in bar, pie, and tabular charts to provide insight into how the system is performing, such as system overview, policies applied, server inventory and status, servers that are associated vs. unassociated, and so on.

  You can add some or all of these reports to your Cisco UCS Director dashboard for quick access.

- **Tabular reports** for detailed information about specific components. They provide the status of the components in a pod. You can export the data from any tabular report in PDF, CSV, or XLS format. If you have scheduled inventory collection, the status is updated regularly. Otherwise, you can click **Refresh** on the tabular report to get real-time status.

You can access tabular reports from any page after you choose the pod. Reports are available for the following components:

- Compute reports
- Storage reports
- Network reports

- **More reports** include Top 5 reports and other reports for detailed information about high-performing resources. You can select the report type to display as tabular, trending, or instant. You can customize some of these reports by choosing the report widget and time duration.

Inventory Collection

When you add a pod, Cisco UCS Director discovers and collects the inventory of that pod. You can view the collected inventory and the status of the pod and its components in the summary reports and on the report pages. This status can be updated on a regular schedule through system tasks and manually by component.

Components You Can Monitor

You can view the inventory, monitor details, and view reports for each component including the following:

- Fabric interconnects
- Chassis and its components, including fan modules, power supply units (PSUs), I/O modules, servers, and decommissioned servers.
- Servers
- Organizations
- Service profiles
- VSANS
- VLANs
- Port channels
- QoS system classes
- Chassis discovery policy
- Management IP pool
- Flow control policies
- Pending Activities
- vMedia Policy
- Locales
- Faults and events

Monitoring a Fabric Interconnect and its Components

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Fabric Interconnects**.

Step 4 Click the row in the table for the fabric interconnect that you want to monitor.

Step 5 Click **View Details**.

Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the fabric interconnect or a specific component in the fabric interconnect:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Summary	Summary of the current status of the fabric interconnect and its components, including CPU utilization and data usage statistics.
Power Supply Units	List of the PSUs with their current status.
Fans	List of the fans in the fabric interconnect with their current status.
Ethernet Ports	List of the Ethernet ports in the fabric interconnect, including their location and current status.
Fibre Channel Ports	List of the Fibre Channel ports in the fabric interconnect, including their location, current status, and associated VSAN.
Events	List of current events for the fabric interconnect and its components, with information about each event.
Faults	List of the current faults for the fabric interconnect and its components, with information about each fault.
More Reports	Additional reports that you can generate for the fabric interconnect and its components, including data usage, CPU utilization, and memory usage reports.

Step 7 To return to the main window, click **Back**.

Monitoring a Chassis and its Components

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Chassis**.

Step 4 Click the row for the chassis that you want to monitor.

Step 5 Click **View Details**.

Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the chassis or a specific component in the chassis:

Name	Description
Summary	Summary of the current status of the chassis and its components.
Servers	List of the servers in the chassis with their location and current status.
Fan Modules	List of the fan modules in the chassis with their current status.
Power Supply Units	List of the PSUs in the chassis with their current status.
Events	List of the current events for the chassis and its components, with information about each event.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
IO Modules	List of the I/O modules in the chassis with their location and current status.
Faults	List of the current faults for the chassis and its components, with information about each fault.
More Reports	Additional reports that you can generate for the chassis and its components, such as an input/output power trend report.

Step 7 To return to the main window, click **Back**.

Monitoring a Server and its Components

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server that you want to monitor.

Step 5 Click **View Details**.

Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the server or a specific component in the server:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Summary	Summary of the current status of the server and its components, including power and temperature statistics.
Interface cards	List of the adapters in the server with their location and current status. To view the DCE interfaces, vNICs, and vHBAs on a adapter, choose the adapter and click **View Details**.
Fan Modules	List of the fan modules in the server with their current status. This tab is only available for rack-mount servers. To view the fans in a fan module, choose the fan module and click **View Details**.
Power Supply Units	List of the PSUs in the server with their current status. This tab is only available for rack-mount servers.
Events	List of the current events for the server and its components, with information about each event.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
Processor Units	List of the CPUs in the server with their location and current status.
Memory Units	List of the memory units in the server with their type, location, and current status.
Storage Controllers	List of the storage controllers in the server.
Faults	List of the current faults for the server and its components, with information about each fault.
Service Request Details	List of the service requests for the server and its components, including the asset type and change description.
More Reports	Additional reports that you can generate for the server and its components, including voltage, power, and temperature reports.

Step 7 To return to the main window, click **Back**.

Monitoring a FEX and its Components

For a Cisco UCS domain that includes one or more rack-mount servers, you can use Cisco UCS Director to monitor each Fabric Extender (FEX) that connects the rack-mount servers to the fabric interconnects.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account

Step 3 Click **FEX**.

Step 4 Click the row for the FEX that you want to monitor.

Step 5 Click **View Details**.

Cisco UCS Director displays information about the current status of the selected component. Click the tabs in the window for more details about that component.

Step 6 Click on one of the following to view the status of the FEX or a specific component in the FEX:

Name	Description
License Status	Overview of the available licenses, the license usage, and any license violations.
Power Supply Units	List of the PSUs with their current status.
Fans	List of the fans in the FEX with their current status.
Suppression Tasks	List of the fault suppression tasks, if any, including the associated policy and schedule.
IO Modules	List of the I/O modules in the FEX with their location and current status.
Faults	List of the current faults for the fabric interconnect and its components, with information about each fault.

Step 7 To return to the main window, click **Back**.

Viewing the Cisco UCS Manager Pending Activities Report and User Acknowledgement

When changes are made to a service profile that is already associated with a server, you must reboot the server to complete the process. The Reboot policy determines when the disruptive changes are implemented. If the maintenance policy is not set to Immediate, all the changes made stay in pending mode until the specified maintenance window or until you acknowledge it explicitly.

This report shows you the **Pending Activities** that are waiting for user acknowledgement, including service profile name, and server affected information.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, choose a **Pod**.

Step 3 Choose a **Cisco UCS Manager Account** under the **Pod**.

Step 4 On the **UCS Manager Account** screen, click the drop-down list at the far right to choose **Pending Activities**.

You can view the activities that are in pending state and require user acknowledgement.

a) Select the pending activity that you want to deploy immediately, and click **Acknowledge** to apply the changes.
b) On the **Acknowledge Pending Activity** screen, click **Acknowledge**.

Cisco UCS Manager immediately reboots the server affected by the pending activity.

After the activity has been acknowledged, it is removed from the pending activities report.

TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M3 and higher blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

Inventory Reports

Viewing Storage Profile Management Reports

Reports are added to Storage Profile, Storage Profile LUN and PCH Controller definitions. Storage Profile data is collected from the Cisco UCS Manager appliance based on the version of the Cisco UCS Manager. If the version is supported, Storage Profile inventory collects the Storage profile related data and the collected data is represented as tabular reports

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Storage Profiles**.

Step 4 From the **Storage Profiles** list, choose the organization.

Step 5 Click **View Details**.

Step 6 Click on either **Local LUNs**, the **PCH Controller Definitions**, or the **Storage Profiles Usage-Service Profiles/Template** to see the respective report.

Viewing the Cisco UCS Chassis Inventory Report

This report shows you the number of chassis in a Cisco UCS Manager account and how many of them are powered on.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **More Reports**.

Step 4 From the **Reports** drop-down list, choose **UCS Chassis Inventory**.

Viewing the Disk Group Policy Inventory Reports

Disk Group Policy data is collected from the Cisco UCS Manager appliance based on the version of the Cisco UCS Manager. If the version is supported, Disk Group Policy inventory collection is done.

The collected data is represented as tabular reports.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **Organizations**.
Step 4 From the **Organizations** list, choose the organization.
Step 5 Click **View Details**.
Step 6 Click **DiskGroup Policy**.
Step 7 From the **DiskGroup Policy** list, choose a disk.
Step 8 Click **View Details**.
Step 9 Click on either the **Virtual Drive** or the **Disk Group** to see the respective report.

Viewing the Cisco UCS Fabric Interconnect Inventory Report

This report shows you the number of fabric interconnects in a Cisco UCS Manager account and how many of them are operable.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **More Reports**.
Step 4 From the **Reports** drop-down list, choose **UCS Fabric Interconnect Inventory**.

Viewing the Cisco UCS Servers Inventory Report

This report shows you the number of Cisco UCS servers in a Cisco UCS Manager account and how many of those servers are operable.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **More Reports**.
Step 4 From the **Reports** drop-down list, choose **UCS Server Inventory**.

Viewing the Cisco UCS Server Association Report

This report shows you the number of associated, unassociated, and other Cisco UCS servers in a Cisco UCS Manager account.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **More Reports**.

Step 4 From the **Reports** drop-down list, choose **UCS Servers Associated vs Unassociated**.

Viewing the vMedia Policy Inventory Report

This report shows you the vMedia Policy distinguished name (DN), description, the retry option for mount failure, policy level, and owner. You can also drill down on the policy report to obtain a list of all the vMedia mounts available under the vMedia policy.

You can also create, edit, or delete a vMedia policy. See Creating a vMedia Policy and vMount.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod with the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Choose the row with the organization for which you want to view the vMedia policy and click **View Details**.

Step 5 Click **vMedia Policy**.

vMedia policies include one or more vMedia mounts. In most cases, there is one vMedia Mount per vMedia Policy. To view the **vMedia Mount** report, select the vMedia Policy and click **View Details**. The report shows you the vMedia mounts for the policy, including distinguished name (DN), mount name, device type, protocol, authentication information, remote server information, remote path, remote filename, and user.

Exporting an Inventory Report

You can export an inventory report in PDF, CSV, or XLS format.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **More Reports**.

Step 4 From the **Reports** drop-down list, choose the report that you want to export.

Step 5 Click**Export Report**.

Step 6 On the **Export Report** screen, choose the desired report format from the **Select Report Format** drop-down list and then click **Generate Report**.

Step 7 After the report has been generated, click **Download**.

Step 8 After you have downloaded the report, click **Close**.

Cisco UCS Events

In Cisco UCS, each event represents a nonpersistent condition in the Cisco UCS domain. After Cisco UCS Manager creates and logs an event, the event does not change. For example, if you power on a server, Cisco UCS Manager creates and logs an event for the beginning and the end of that request.

You can view all events in a Cisco UCS Manager account from Cisco UCS Director. You can view Cisco UCS events for individual Cisco UCS Manager accounts or for specific components in the account, such as a server or fabric interconnect.

Viewing Cisco UCS Events for a Cisco UCS Manager Account

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Events**.

Step 4 (Optional) To view events for a component within the account, do the following:

a) Navigate to the component, such as servers or fabric interconnects.
b) Click on the row for the component for which you want to view events.
c) Click **View Details**.
d) Click **Events**.

Step 5 (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.
b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

Step 6 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Cisco UCS Faults

Each Cisco UCS fault represents a failure in the Cisco UCS domain or an alarm threshold that has been raised. During the lifecycle of a fault, it can change from one state or severity to another.

Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, the object transitions to a functional state.

You can view all faults in a Cisco UCS Manager account from Cisco UCS Director. You can also view Cisco UCS faults at the pod level, either for individual Cisco UCS Manager accounts or for specific components in the account.

For more information about Cisco UCS faults, see the Cisco UCS Faults and Error Messages Reference and the Cisco UCS Manager B-Series Troubleshooting Guide.

Viewing Cisco UCS Faults for a Pod

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Faults**.

Step 4 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Viewing Cisco UCS Faults for a Cisco UCS Manager Account

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Faults**.

Step 4 (Optional) To view faults for a component or object within the account, do the following:

a) Navigate to the component or object, such as service profiles, servers, or organizations.
b) Click on the row in the table for the component or object for which you want to view faults.
c) Click **View Details**.
d) Click the **Faults**.

Step 5 (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.
b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

Step 6 (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.
b) In the **Export Report** dialog box, select a report format and click **Generate Report**.
c) When the report has generated, click **Download**.
d) If the report opens in a separate tab, use the download button from your browser to download the report.
e) In the **Export Report** dialog box, click **Close**.

Fault Suppression

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Director sends notifications for any outstanding suppressed faults that have not been cleared.

Adding a Fault Suppression Task for a Chassis

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Chassis**.

Step 4 Click the row for the chassis for which you want to suppress faults.

Step 5 Click **Start/Stop Fault Suppression**.

Step 6 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 7 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval**—Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule**—Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.

Name	Description
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This can be one of the following: • **default-server-maint**—Suppresses faults for blade servers. • **default-iom-maint**—Suppresses faults for IOMs in a chassis. • **default-chassis-all-maint**—Suppresses faults for the chassis and all components installed into the chassis, including all blade servers, power supplies, fan modules, and IOMs. • **default-chassis-phys-maint**—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis.

Repeat this step to add additional fault suppression tasks.

Step 8 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for a FEX

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **FEX**.

- **Chassis** tab
- **FEX** tab

Step 4 Click the row in the table for the FEX for which you want to suppress faults.

Step 5 Click the row for the Chassis or FEX for which you want to suppress faults on an I/O module and click **View Details**.

Step 6 Click **Start/Stop Fault Suppression**.

Step 7 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 8 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.

Name	Description
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval**—Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule**—Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This can be one of the following: • **default-fex-phys-maint**—Suppresses faults for the FEX and all fan modules and power supplies in the FEX. • **default-fex-all-maint**—Suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX. • **default-iom-maint**—Suppresses faults for IOMs in the FEX.

Repeat this step to add additional fault suppression tasks.

Step 9 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for an I/O Module

You can suppress faults on an I/O module in a FEX or chassis.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **Chassis** tab
- **FEX** tab

Step 4 Click the row for the Chassis or FEX for which you want to suppress faults on an I/O module and click **View Details**.

Step 5 Click **IO Modules**.

Step 6 Click the row for the I/O module for which you want to suppress faults.

Step 7 Click **Start/Stop Fault Suppression**.

Step 8 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 9 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval**—Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule**—Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the predefined suppression policy to be applied to this task. This policy is **default-iom-maint**, which suppresses faults for IOMs in a chassis or FEX.

Repeat this step to add additional fault suppression tasks.

Step 10 When you have added all fault suppression tasks, click **Submit**.

Adding a Fault Suppression Task for a Server

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **UCS Servers**.

Step 4 Click the row for the server for which you want to suppress faults.

Step 5 Click **Start/Stop Fault Suppression**.

Step 6 On the **Fault Suppression** screen, expand **Locally Defined Suppression Tasks** and click **Add**.

Step 7 On the **Add Entry to Locally Defined Suppression Tasks** screen, complete the following fields and click **Submit**:

Name	Description
Name field	A unique name for the fault suppression task.

Name	Description
Select Fixed Time Interval/Schedule drop-down list	Choose when the fault suppression task will run. This can be one of the following: • **Fixed Time Interval**—Specifies the start time and duration for the fault suppression task. Specify the day and time that the fault suppression task should start in the **Start Time** field. Click the calendar icon at the end of this field to choose the start time from a pop-up calendar. Specify the length of time that this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule**—Configures the start time and duration using a predefined schedule. Choose the schedule from the **Schedule** drop-down list.
Suppression Policy drop-down list	Choose the pre-defined suppression policy to be applied to this task. This policy can be **default-server-maint**, which suppresses faults for blade and rack-mount servers.

Repeat this step to add additional fault suppression tasks.

Step 8 When you have added all fault suppression tasks, click **Submit**.

Viewing Fault Suppression Tasks

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click one of the following:

- **Chassis**
- **FEX**
- **UCS Servers**

Step 4 Click the row for the chassis, FEX, or server for which you want to view fault suppression tasks and click **View Details**.

Step 5 Click **Suppression Tasks**.