Monitoring and Reporting

About Monitoring and Reporting

Cisco UCS Director displays all managed components in each rack-mount server that has been added to a rack group. These components can be hardware or software.

Information You Can View

You can view and monitor details about each component, including the following:

- License status
- Summary of the current status

Components You Can Monitor

You can monitor specific components or view reports for each of the components, including the following:

- vNICs and vHBAs
- Adapters, such as network and PCI
- Hardware components, such as CPUs, interface cards, and memory

Email Alerts

You can configure rules in Cisco UCS Director so that an email message is triggered when faults of a certain severity occur on rack servers or rack server groups. When fault conditions specified in the rule occur, an email message is triggered and sent to the recipients you have specified. For information on configuring these email alert rules, see Configuring Email Alert Rules, on page 4.

Monitoring a Rack Server and Its Components

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of the server that you want to monitor.

Step 5 Click **View Details**.
By default, the **Summary** tab is displayed.

Step 6 Click on one of the tabs to view the status of the licenses, the server, or a specific component in the server.
Additional information may be available if you click **View Details** on one or more of the individual components.

Viewing Reports About a Rack Server

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group and then choose the rack server group.

Step 3 In the right pane, click the **Rack Server** tab.

Step 4 Choose the row of the server for which you want to view reports.

Step 5 In the right pane, click the **Summary** tab to view a wide array of tabular, graphical, and map reports that provide a view of trending data for the account.

Step 6 For some reports, you can click the icons on the table bar to customize the table columns, filter the results, or export a report of the current table contents.
For more information, see the Cisco UCS Director Administration Guide.

Clearing SEL

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

Step 3 In the right pane, click the **Rack Servers** tab.

Step 4 Double-click the sever from the list to view the details or click the sever from the list and click the down arrow on the far right and choose **View Details**.

Step 5 Click the **System Event Log** tab.

Step 6 Click **Clear IMC SEL Log**.

Step 7 (Optional) In the **Clear IMC SEL Logs** dialog box, check the **Delete historical logs from Cisco UCS Director** check box.
Selecting this option clears the system event logs from the Cisco UCS Director GUI.

Step 8 Click **Submit**.

Uploading Technical Support Data to a Server

Procedure

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod that contains the rack server group, and then choose the rack server group.

Step 3 In the right pane, click the **Rack Servers** tab.

Step 4 Double-click the sever from the list to view the details or click the sever from the list and click the down arrow on the far right and choose **View Details**.

Step 5 Click the **Tech Support** tab.

Step 6 Click **Create Tech Support**.

Step 7 In the **Create Tech Support** dialog box, complete the following fields:

Name	Description
Destination Type drop-down list	Select a destination for the support data. It can be one of the following: • Remote—Implies an external server • Local—Implies the current system.

Name	Description
Network Type drop-down list	The network type. This can be one of the following: • **TFTP** • **FTP** • **SFTP** • **SCP**
Server IP/Hostname field	The IP address or hostname of the server on which the support data file should be stored. Depending on the setting in the **Network Type** drop-down list, the name of this field will vary.
Path and Filename field	The path and filename that must be used when uploading the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the network type is TFTP.
Password	The password for the remote server username. This field does not apply if the network type is TFTP.

Step 8 Click **Submit**.

Configuring Email Alert Rules

Procedure

Step 1 On the menu bar, choose **Administration** > **System**.

Step 2 Choose the **Email Alert Rules** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Add Email Alert Rule** dialog box, complete the following fields:

Field	Description
Name field	A unique name for the email alert rule.
Alert Scope drop-down list	Choose if the alert rule applies to a system, server groups or servers.

Field	Description
Server Groups field	Click **Select** to check the check boxes of the server groups that email alerts should be sent for. This field is displayed only when **Server Group** is selected in the **Alert Scope** drop-down list.
Servers field	Click **Select** to check the check boxes of the servers that email alerts should be sent for. This field is displayed only when **Server** is selected in the **Alert Scope** drop-down list.
Email Address field	The email address of the recipients of the email. You can enter multiple email addresses, separated by commas.
Severity field	Click **Select** to check the check boxes of the severity levels for which the email alert must be triggered.
Enable Alert check box	Check this check box to enable the alert rule immediately.

Step 5 Click **Submit**.

Server Diagnostics

Overview of Server Diagnostics

Server diagnostics is available through UCS Server Configuration Utility (UCS-SCU). You can use diagnostics tools to diagnose hardware problems with your Cisco servers and run tests on various server components to find out hardware issues along with analysis of the test results in a tabular format.

You must download, configure, and save the UCS-SCU image to a remote location.

Note Running a diagnostic test using the UCS-SCU image results in the server being temporarily unavailable as the server reboots with the UCS-SCU image.

When you run diagnostics on any rack server, it reboots with the UCS-SCU image hosted on the location you have configured. The diagnostics tabular report displays the status of diagnostics for each server on which you have run diagnostics. Also, details of the server, the date and time the report was generated, diagnostics status and so on are displayed. You can delete or download diagnostic reports for a single or for multiple servers.

Note You must configure the scpuser password to run server diagnostics. To configure the scpuser password, see Configuring an SCP User Password, on page 7.

Configuring Server Configuration Utility Image Location

Perform this procedure to configure and save the location of the UCS-SCU image.

Procedure

Step 1 On the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Choose the **SCU Image Profiles** tab.

Step 3 Click **Add**.

Step 4 In the **Configure SCU Image Location** dialog box, complete the following:

Field	Description
Profile Name field	Enter a name for the SCU image profile.
ISO Share Type drop-down list	Choose either Network File System (NFS), Common Internet File System (CIFS), World Wide Web (WWW) or Local share type.
ISO Share IP field	Enter the ISO share IP address.
ISO Share Path field	Enter the ISO share path.
Username field	Enter your ISO share login user name.
Password field	Enter your ISO share login password.

Step 5 Click **Save**.

Step 6 In the **Submit Result** dialog box, click **OK**.

Running Diagnostics

Perform this procedure when you want to run diagnostics for servers or server groups. Running diagnostics on servers will result in the selected servers being restarted.

Procedure

Step 1 On the menu bar, choose **Administration** > **Physical Accounts**.

Step 2 Choose the **Server Diagnostics** tab.

Step 3 Click **Run Diagnostics**.

Step 4 In the **Run Diagnostics** dialog box, complete the following:

Field	Description
Select Profile drop-down list	Choose a diagnostics profile from the list.
Server(s) drop-down list	Click **Select** to check the check boxes of the server groups for which you want to run the diagnostics.

Step 5 Click **Submit**.

Note You can perform the following actions on a server or multiple servers:

- Select a server and click **View Report** to view reports.
- Select a server or multiple servers and click **Delete Report** to delete reports.
- Select a server or multiple servers and click **Download Report** to download reports. When you select multiple servers to download diagnostics reports, a zip file containing all the reports are downloaded.

You cannot choose a server which is already running a diagnostics operation. Wait for the diagnostics operation to complete before triggering another diagnostics on this server.

Diagnostics may take around 40 minutes to complete. This varies depending on the number of components present in the server.

Configuring an SCP User Password

An SCP user is used by server diagnostics and tech support upload operations for transferring files to the Cisco IMC Supervisor appliance using the SCP protocol. An scp user account cannot be used to login to the Cisco IMC Supervisor UI or the shelladmin. You must create an SCP user using Putty, and then log in to the user interface to set a password.

Complete this procedure to configure a password for an SCP user.

Procedure

Step 1 From the menu bar, choose **Administration** > **Users and Groups**.

Step 2 Click the **SCP User Configuration** tab.

Step 3 Enter the scp user password in the **Password** field.

Step 4 Click **Submit**.

Step 5 In the **Submit Result** dialog box, click **OK**.