Configuring Statistics-Related Policies

This chapter includes the following sections:

Configuring Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the blade chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Modifying a Statistics Collection Policy

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All ➤ Stats Management ➤ Stats**.

Step 3 Right-click the policy that you want to modify and select **Modify Collection Policy**.

Step 4 In the **Modify Collection Policy** dialog box, complete the following fields:

Name	Description
Collection Interval field	The length of time the fabric interconnect should wait between data recordings. This can be: • **30 Seconds** • **1 Minute** • **2 Minutes** • **5 Minutes**
Reporting Interval field	The length of time the fabric interconnect should wait before sending any data collected for the counter to Cisco UCS Manager GUI. This can be: • **15 Minutes** • **30 Minutes** • **60 Minutes** When this time has elapsed, the fabric interconnect groups all data collected since the last time it sent information to Cisco UCS Manager GUI, and it extracts four pieces of information from that group and sends them to Cisco UCS Manager GUI: • The most recent statistic collected • The average of this group of statistics • The maximum value within this group • The minimum value within this group

Name	Description
	For example, if the collection interval is set to 1 minute and the reporting interval is 15 minutes, the fabric interconnect collects 15 samples in that 15 minute reporting interval. Instead of sending 15 statistics to Cisco UCS Manager GUI, it sends only the most recent recording along with the average, minimum, and maximum values for the entire group.
States Section	
Current Task field	This field shows the task that is executing on behalf of this component. For details, see the associated **FSM** tab. **Note** If there is no current task, this field is not displayed.

Step 5 Click **OK**.

Configuring Statistics Threshold Policies

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the BMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Creating a Server and Server Component Threshold Policy

Tip This procedure documents how to create a server and server component threshold policy on the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Threshold Policies** and select **Create Threshold Policy**.

Step 5 In the **Define Name and Description** page of the **Create Threshold Policy** wizard, do the following:

a) Complete the following fields:

Name	Description
Name field	The name assigned to the threshold policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the threshold policy.

b) Click **Next**.

Step 6 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Choose Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ethernet-port-stats-by-size-large-packets**
- **ethernet-port-stats-by-size-small-packets**
- **ethernet-port-err-stats**
- **ethernet-port-multicast-stats**
- **ethernet-port-over-under-sized-stats**
- **ethernet-port-stats**
- **fc-port-stats**
- **vnic-stats**
- **cpu-stats**

- **dimm-stats**
- **mb-power-stats**
- **mb-temp-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in an organization.

c) Click **Next**.

Step 7 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, select the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 7.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 8 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 6 and 7.

- If you have configured all required threshold classes for the policy, click **Finish**.

Step 9 Click **OK**.

Adding a Threshold Class to a Server and Server Component Threshold Policy

Tip This procedure documents how to add a threshold class to a server and server component threshold policy in the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Policies** ➤ ***Organization_Name***.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click the policy to which you want to add a threshold class and select **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ethernet-port-stats-by-size-large-packets**
- **ethernet-port-stats-by-size-small-packets**
- **ethernet-port-err-stats**
- **ethernet-port-multicast-stats**
- **ethernet-port-over-under-sized-stats**
- **ethernet-port-stats**
- **fc-port-stats**
- **vnic-stats**
- **cpu-stats**
- **dimm-stats**
- **mb-power-stats**
- **mb-temp-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in an organization.

c) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, select the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes:
st fo the

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

h) Click **Finish Stage**.

i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Step 8 Click **OK**.

Deleting a Server and Server Component Threshold Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** ➤ **Policies** ➤ ***Organization_Name***.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy

Tip You cannot create an uplink Ethernet port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** ➤ **LAN Cloud**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and select the **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **ether-error-stats**
- **ether-loss-stats**
- **ether-rx-stats**
- **ether-tx-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **LAN Cloud** node.

c) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, select the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes: st fo the
g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy

Tip You cannot create an Ethernet server port, chassis, and fabric interconnect threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 In the **LAN** tab, expand **LAN** ➤ **Internal LAN**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and select the **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page, do the following:

a) Click **Add**.

b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **chassis-stats**
- **fan-module-stats**
- **fan-stats**
- **io-card-stats**
- **psu-input-stats**
- **psu-stats**
- **ether-error-stats**
- **ether-loss-stats**
- **ether-rx-stats**
- **ether-tx-stats**
- **env-stats**
- **system-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **Internal LAN** node.

c) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, select the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**

- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes: st fo the
g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Fibre Channel Port Threshold Policy

You cannot create a Fibre Channel port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN ➤ SAN Cloud**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and select the **Create Threshold Class**.

Step 5 In the **Create Threshold Class** page, do the following:

a) Click **Add**.
b) In the **Statistics Class** dialog box, select one of the following classes to configure from the **Stat Class** drop-down list:

- **fc-error-stats**
- **fc-stats**

Note If you see a different list of statistics classes, verify that you are creating the threshold policy in the **SAN Cloud** node.

c) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.
b) From the **Property Type** field, select the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes: st fo the

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

h) Click **Finish Stage**.

i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.