Creating Monitoring Policies and Thresholds

Prime Infrastructure uses monitoring policies to monitor devices against the thresholds you specify. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm. The alarms warn you of changing conditions before the issues impact operations.

By default, Prime Infrastructure polls:

- Device health metrics on supported routers, switches and hubs. Storage devices and UCS series devices are not monitored by the default health policy. See Modifying Default Monitoring Policies.
- Port group health metrics.
- Interface health metrics on WAN interface groups, AVC, and UCS.

Note Prime Infrastructure uses monitoring policies only for Wired devices.

You can also enable other Prime Infrastructure monitoring policies or create a custom MIB polling policy (see Monitoring Third-Party Devices By Polling MIBs).

Default Monitoring Policies

Prime Infrastructure polls SNMP objects to gather monitoring information for the following health monitoring policies under **Monitor > Monitoring Tools > Monitoring Policies > Automonitoring**:

- Device Parameters—Table 10-1 describes the device health parameters that are polled.
- Interface Parameters—Table 10-2 describes the interface parameters that are polled for:
  - Trunk and Link Ports
  - WAN Interfaces

For the following monitoring policies that provide assurance information, data is collected through NetFlow or NAMs:

- Application Response Time
- NAM Health
- Traffic Analysis
- Voice Video Data
- Voice Video Signaling

Table 10-1 Device Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Device Availability	All SNMP devices	SNMPv2-MIB	sysUpTime
CPU Utilization	Cisco IOS devices, All Supported Nexus devices, Cisco UCS devices	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
Memory Pool Utilization	Cisco IOS devices	CISCO-MEMORY-POOL-MIB ciscoMemoryPoolUsed / (ciscoMemoryPoolUsed + ciscoMemoryPoolFree)) * 100	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	All supported Cisco Nexus devices, Cisco UCS devices	CISCO-MEMORY-POOL-MIB (cempMemPoolUsed / (cempMemPoolUsed + cempMemPoolFree)) * 100	
Environment Temp[1]	ASR, All Supported Nexus devices, Cisco UCS devices	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000, 3000, 4000, 6000, ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

1. For stacked switch devices, the Environment Temp displays the temperature of each stacked instance.

Table 10-2 Interface Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Interface Availability	Cisco IOS devices, All Supported Nexus devices	IF-MIB	ifOperStatus ifOutOctets ifHighSpeed ifInOctets ifInErrors ifOutErrors ifInDiscards ifOutDiscards
Input Utilization	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts

Table 10-2 Interface Parameter Automonitoring Metrics (continued) (continued)

Metric	Devices Polled	MIB	MIB Objects Included
Output Utilization	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifHCInUcastPkts, ifInDiscards, ifInUnknownProtos, locIfInputQueueDrops
Percent Drop per QoS Class	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops

Table 10-3 Class-Based, QoS, Health-Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
QOS calculation	Cisco IOS devices	CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64
Interface Inbound Errors	Cisco IOS devices	IF-MIB	ifInErrors
Interface Outbound Errors	Cisco IOS devices	IF-MIB	ifOutErrors
Interface Inbound Discards	Cisco IOS devices	IF-MIB	ifInDiscards
Interface Outbound Discards	Cisco IOS devices	IF-MIB	ifOutDiscards

Modifying Default Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation. By default, Prime Infrastructure polls device health metrics on supported routers, switches and hubs only, and interface health metrics on WAN interface groups. It is not polled on storage devices, and UCS series devices. If a the threshold is violated three times, Prime Infrastructure generates a critical alarm, which is displayed on the **Monitor > Monitoring Tools > Alarms and Events** page.

To modify or disable the polling frequency and the threshold parameters, follow these steps:

Step 1 Choose **Monitor > Monitoring Tools > Monitoring Policies > Automonitoring**.

Step 2 Select **Device Health**, then modify the polling frequencies and thresholds as desired.

Step 3 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

Creating New Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation.

To create a new monitoring policy, follow these steps:

Step 1 Choose **Monitor > Monitoring Tools > Monitoring Policies > My Policies**.

Step 2 Click **Add**.

Step 3 Select a monitoring policy from the Policy Types menu.

Step 4 Enter a name for the new policy.

Step 5 Under Parameters and Thresholds, specify the threshold values for which you want Prime Infrastructure to issue an alarm when they are reached.

Step 6 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

Monitoring Third-Party Devices By Polling MIBs

You can design custom MIB polling policies to monitor third-party or Cisco devices and device groups. You can also create custom MIB policies to monitor device features for which Prime Infrastructure doesn't provide default policies. Using this feature, you can:

- Upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency.
- Upload a single MIB definition file or a group of MIBs with their dependencies as a ZIP file.

Note Ensure that you upload all the dependencies of the MIB, before uploading the MIB. You can also upload the MIB along with it's dependencies in a ZIP file.

- Display the results as a line chart or a table.

This feature allows you to easily repeat polling for the same devices and attributes and customize the way Cisco devices are polled using SNMP.

You can create a maximum of 25 custom MIB polling policies. There is no limitation in the number of MIB files uploaded.

To create custom MIB polling policies, follow these steps:

Step 1 Choose **Monitor > Monitoring Tools > Monitoring Policies > My Policies**, then click **Add**.

Step 2 From the Policy Types menu, select **Custom MIB Polling**.

Step 3 Enter a name for the policy.

Step 4 Under the MIB Selection tab, specify the polling frequency and enter the MIB information.

- If Prime Infrastructure doesn't have the specific MIB you want to monitor, download the MIBs you want to monitor from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2
- To upload a MIB, specify a filename extension only if you are uploading a ZIP file.

  Regardless of the device, the extensions .ZIP,.MIB and .MY are allowed.
- If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
- Ensure your upload file and the MIB definition have the same name (for example: Do not rename the ARUBA-MGMT-MIB definition file to ARUBA_MGMT). If you are uploading a ZIP file, you may name it as you please, but the MIB files packaged inside it must also follow this convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).

Step 5 To test the policy you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.

Step 6 Click **Save and Activate** to immediately activate the policy on the devices specified.

Step 7 To view the MIB polling data, create a generic dashlet (see Creating Generic Dashlets) using the name of the policy that you created.

To view the SNMP polling date for ASR devices, you should use the s**how platform hardware qfp active datapath utilization | inc Processing** command for CPU utilization and **show platform hardware qfp active infrastructure exmem statistics | sec DRAM** command for memory utilization.

Example: Monitoring IP SLA

You can create a monitoring policy to view IP service levels for network-based applications and services. There are approximately seven IP SLA-related MIBs. In this example, the video MIB only is monitored.

Step 1 Download the IP SLA video MIB from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2

Step 2 Choose **Monitor > Monitoring Policies > My Policies**, then click **Add**.

Step 3 Click **Custom MIB Polling**.

Step 4 Enter a name for the policy.

Step 5 Under the MIB Selection tab, click **Upload MIB** and navigate to the MIB that you uploaded in Step 1.

Step 6 From the Tables pulldown menu, select a table, then select the specific metrics to monitor.

Step 7 To test the policy you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.

Step 8 Select the devices for which you want to monitor IP SLA metrics.

Step 9 Click **Save and Activate** to immediately activate the policy on the devices specified.

Step 10 To monitor this information from a dashboard, you need to create a generic dashlet. See Creating Generic Dashlets for more information.

Polled Data in Dashlets and Reports

When viewing polled data from devices, consider the following scenario:

- Device 1 data is polled from the last 6 hours.
- Device 2 data is polled from the last 2 days.

When you filter dashlets or reports to show data from the past 2 days, only the data from Device 2 is displayed.

If you filter dashlets and reports by devices and time frame, then data for both devices is displayed.