Using Passive Monitors

Unlike active monitors or performance monitors, which actively poll a device to check its status or to gather statistical data, passive monitors passively listen for events on devices.

Because it does not repeatedly poll devices and wait for a device to signal a problem, a passive monitor uses fewer resources than an active monitor both on the machine running Cisco netManager and on the network.

Passive monitors are also useful because some devices on a network may not provide a clear up or down status when queried. For example, a message may get logged to the system's Event log by another application (such as an antivirus application alerting when a virus is found). Since these messages or events can occur at any time, a Passive Monitor Listener listens for them, and notifies Cisco netManager when they occur.

However, the information that can be reported in a passive monitor event is not as customizable as it is with active monitors. In the case of a severe device failure, a device may enter a state where it is not able to successfully send a passive monitor event. A connectivity loss may prevent the Cisco netManager system from receiving an event sent to it as well.

Passive monitors should be used to complement active monitors, but you should not rely solely on passive monitors to monitor a device or service.

The first step in using this function is to configure the Passive Monitor Listeners. For more information, see Configuring Passive Monitor Listeners, page 9-1. After the listeners have been configured, you can Configure passive monitors for individual devices. For more information, see Adding or Editing Passive Monitors, page 9-2.

Passive Monitors Icon

When a passive monitor is configured on a device, the device icon displays a diamond shape on the upper left side. This shape changes color when an unacknowledged state change occurs on the monitor. After the device has been acknowledged, the icon returns to the previous color.

Configuring Passive Monitor Listeners

A Passive Monitor Listener listens for an event to occur and then notifies Cisco netManager. This lets you get notification of an event when it occurs, rather than requiring you to poll for all event types. The Passive Monitor Listener is solely responsible for how it monitors its events. This means that the server could listen for network traffic or application-specific events.

Cisco netManager is installed with three Passive Monitor Listeners:

- **SNMP Passive Monitor (SNMP Trap)**—A trap is an unsolicited SNMP message sent from a device to indicate a change in status, such as a router indicating one of its interfaces went down or a printer indicating that it is out of paper.

- **Syslog Passive Monitor**—A syslog monitor is used to examine Syslog messages forwarded from other devices for a specific record and/or specific text within a record. Usually Syslog messages are forwarded from the Syslog on a system that runs UNIX, but they can also come from non-UNIX devices as well. They could contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.

- **Windows Event Log Monitor**—This could be monitoring when a service is started or stopped, if there was a logon failure recorded, or any other entry in the Windows Event log

Using the Passive Monitor Library

The Passive Monitor Library dialog displays the passive monitor types that have been created for Cisco netManager. These types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the Monitor types have been configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.

Step 1 From the Cisco netManager web interface, click **GO > Configure > Passive Monitor Library**.

or

From the main menu bar of the Cisco netManager console, click **Configure > Passive Monitor Library**.

Step 2 Click **New** to create a new passive monitor type.

Step 3 Select a monitor type in the list, then click **Edit** to change the settings.

Step 4 Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.

Step 5 Select a monitor type, then click **Delete** to remove it from the list.

Adding or Editing Passive Monitors

To add/edit a passive monitor:

Step 1 From the Cisco netManager web interface, click **GO > Configure > Passive Monitor Library**.

Step 2 Do one of the following:

- Click **New** to configure a new passive monitor.

- Select a monitor from the list, then click **Edit** to make changes to an existing configuration. The configuration dialog for the selected monitor type opens.

Step 3 After you make the necessary changes, click **OK** to add the monitor to the list or to save the changes you made to a monitor already on the list.

Assigning a Passive Monitor to a Device

Step 1 Right-click the device to which you want to assign a passive monitor, then click **Properties**. The Device Properties dialog opens.

Step 2 Click **Passive Monitors**. The Device Properties Passive Monitor dialog opens.

Step 3 Click **Add**. The Passive Monitor Properties dialog opens.

Step 4 Select the passive monitor type and passive monitor you want to assign, then click **Next**. The Setup Actions for Passive Monitors dialog opens.

Step 5 Click **Add** to set up a new action for the passive monitor. The Select or Create Action dialog opens. Click one of the following:

- Select an action from the Action Library
- Create a new action

Step 6 Click **Finish** to add the passive monitor to the device.

Accessing Group and Device Passive Monitor Reports

The following reports display information for devices or device groups that have passive monitors configured and enabled. Access these reports from the web interface Reports tab. For more information, see Chapter 11, "Using Reports."

- SNMP Trap log
- Syslog Entries
- Windows Event log
- Passive Monitor Error log

Receiving SNMP Traps

Cisco netManager has an internal SNMP trap handler, which, when enabled, listens for and accepts SNMP traps that are addressed to it. Cisco netManager records the trap in the device's SNMP Trap log.

You can also set up Cisco netManager to fire an action when a trap is received for a device.For more information, see Using the Trap Definition Import Tool, page 12-4.

To configure Cisco netManager to receive traps:

Step 1 On the devices that will be monitored, set the SNMP agent to send traps to Cisco netManager. Trap manager addresses must be set on each physical device. This cannot be done from Cisco netManager.

Step 2 Set up the MIB entries for traps by placing the MIB text file in the `Mibs` directory.

Step 3 Enable the SNMP Trap Handler

a. From the Cisco netManager console, select **Configure > Program Options**.

b. Select **Passive Monitor Listeners**.

c. Select **SNMP Trap**.

    d. Click the **Configure** button.

    e. Select the appropriate options:

- **Listen for messages on port**. Select this option if you want Cisco netManager to listen for SNMP traps. The standard SNMP trap port is 162, but you can change this port to a nonstandard number. The changes are immediate, and you do not have to restart Cisco netManager for the changes to be in effect.

- **Accept unsolicited SNMP traps**. If this is not selected, *only* traps which are specifically added to devices as events are logged to the activity log and are able to trigger alerts. You may prefer to select this option so that *all* traps which occur can be detected and logged to the activity log. Note that regardless of this filter setting, traps are logged to the SNMP Trap log. By default there is no strict filtering of traps; this way you can see all traps from all sources, then make decisions about creating Actions based on specific traps you have seen. Later you may make the decision to filter out all traps except those you expect to see.

- **Forward traps**. Select this option to forward traps to IP addresses added to the **Forward traps to** list.

- **Forward unsolicited traps**. Select this option to forward all traps, including unsolicited traps.

- **Forward traps to**. Click **Add** to add an IP address and port to forward traps to. You can forward traps to multiple IP addresses.

    f. Click **OK** to save changes.

Note   Installing the SNMP agent on the Cisco netManager machine also starts an SNMP trap service. This can result in a port conflict, because both the SNMP trap service and the Cisco netManager SNMP trap handler listen on port 162. To eliminate this problem, you need to disable the SNMP trap service.