



Monitoring Performance

This chapter describes how to configure Performance Monitoring tools for Cisco DCNM-SAN and Device Manager. These tools provide real-time statistics as well as historical performance monitoring.

This chapter contains the following sections:

- [Information About Performance Monitoring, on page 1](#)
- [Configuring Performance Manager, on page 2](#)
- [Configuring the Summary View in Device Manager, on page 4](#)
- [Configuring Per Port Monitoring using Device Manager, on page 4](#)
- [Viewing Performance Statistics Using DCNM-SAN, on page 4](#)
- [Displaying Performance Manager Reports, on page 5](#)
- [Generating Performance Manager Reports, on page 6](#)
- [Exporting Data Collections , on page 9](#)
- [Analyzing SAN Health, on page 11](#)

Information About Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. Real-time performance statistics are useful for dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in DCNM-SAN and Device Manager. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data.

Real-Time Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.

Device Manager checking for oversubscription on the host-optimized four-port groups on relevant modules. Right-click the port group on a module and choose Check Oversubscription from the pop-up menu.

Device manager provides two performance views: the Summary View tab and the configurable monitor option per port.

Historical Performance Monitoring

Performance Manager gathers network device statistics historically and provides this information using DCNM-SAN client and web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

Configuring Performance Manager

This section includes the following topics:

Creating a Flow with Performance Manager

With the Flow Configuration Wizard you can create host-to-storage, storage-to-host, or bidirectional flows. Once defined, you can add these flows to a collection configuration file to monitor the traffic between a host/storage element pair. The flows created become part of the collection options in the Performance Manager Configuration Wizard.

Creating a Collection with Performance Manager

The Performance Manager Configuration Wizard steps you through the process of creating collections using configuration files. Collections are defined for one or all VSANs in the fabric. Collections can include statistics from the SAN element types described in [Table 1: Performance Manager Collection Types, on page 2](#).

Table 1: Performance Manager Collection Types

Collection Type	Description
ISLs	Collects link statistics for ISLs.
Host	Collects link statistics for SAN hosts.
Storage	Collects link statistics for a storage elements.
Flows	Collects flow statistics defined by the Flow Configuration Wizard.

Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page.

You must choose either absolute value thresholds or baseline thresholds that apply to all transmit or receive traffic defined in the collection. Click the **Use absolute values** radio button on the last screen of the Performance Manager Configuration Wizard to configure thresholds that apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the

threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.

As an example, the collection has absolute value thresholds set for 60% utilization (for warning) and 80% utilization (for critical). If Performance Manager detects that the traffic on a 1-Gigabit link in its collection exceeds 600 Mbps, a warning event is triggered. If the traffic exceeds 800 Mbps, a critical event is triggered.

Baseline thresholds are defined for a configured time of day or week (1 day, 1 week, or 2 weeks). The baseline is created by calculating the average of the statistical results for the configured time each day, week, or every 2 weeks. [Table 2: Baseline Time Periods for a Collection Started on Wednesday at 4pm, on page 3](#) shows an example of the statistics used to create the baseline value for a collection defined at 4 pm on a Wednesday.

Table 2: Baseline Time Periods for a Collection Started on Wednesday at 4pm

Baseline Time Window	Statistics Used in Average Calculation
1 day	Every prior day at 4 pm
1 week	Every prior Wednesday at 4 pm
2 weeks	Every other prior Wednesday at 4 pm

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every 2 weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated average.

As an example, a collection is created at 4 pm on Wednesday, with baseline thresholds set for 1 week, at 150% of the average (warning) and 200% of the average (critical). Performance Manager recalculates the average for each link at 4 pm every Wednesday by taking the statistics gathered at that time each Wednesday since the collection started. Using this as the new average, Performance Manager compares each received traffic statistic against this value and sends a warning or critical event if the traffic on a link exceeds this average by 150% or 200% respectively.

[Table 3: Example of Events Generated for 1-Gigabit Links, on page 3](#) shows two examples of 1-Gigabit links with different averages in our example collection and at what traffic measurements the Warning and Critical events are sent.

Table 3: Example of Events Generated for 1-Gigabit Links

Average	Warning Event Sent at 150%	Critical Event Sent at 200%
400 Mbps	600 Mbps	800 Mbps
200 Mbps	300 Mbps	400 Mbps

Set these thresholds on the last screen of the Collections Configuration Wizard by checking the **Send events if traffic exceeds threshold** check box.

Configuring the Summary View in Device Manager

- Step 1** Click the **Summary** tab on the main display.
You see all of the active ports on the switch, as well as the configuration options available from the Summary view.
- Step 2** Choose a value from the Poll Interval drop-down list.
- Step 3** Decide how you want your data to be interpreted by looking at the Show Rx/Tx drop-down menu. The table updates each polling interval to show an overview of the receive and transmit data for each active port on the switch.
- Step 4** Select a value from the **show Rx/Tx** drop-down list. If you select **Util%**, you need to also select values from the two **Show Rx/Tx > %Util/sec** drop-down lists. The first value is the warning level and the second value is the critical threshold level for event reporting.
- Note that you can also display percent utilization for a single port by selecting the port and clicking the Monitor Selected Interface Traffic Util % icon.
-

Configuring Per Port Monitoring using Device Manager

The configurable monitor per port option gives statistics for in and out traffic on that port, errors, class 2 traffic and other data that can be graphed over a period of time to give a real-time view into the performance of the port.

- Step 1** Click the **Device** tab.
- Step 2** Right-click the port you are interested in and choose Monitor from the drop-down menu.
You see the port real-time monitor dialog box.
- Step 3** Select a value from the Interval drop-down list to determine how often data is updated in the table shown here.
- Step 4** Click a statistical value in the table then click one of the graphing icons to display a running graph of that statistic over time. You see a graph window that contains options to change the graph type.
- Tip** You can open multiple graphs for statistics on any of the active ports on the switch.
-

Viewing Performance Statistics Using DCNM-SAN

You can configure DCNM-SAN to gather historic and real time statistics of ISLs or End devices. These statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL or end device.

SUMMARY STEPS

1. Right-click the ISL or end device in the Fabric pane.
2. Select Show Statics.

DETAILED STEPS

Step 1 Right-click the ISL or end device in the Fabric pane.

You see a context menu.

Step 2 Select Show Statics.

Note Show Statics menu will be enabled only if you add the fabric to the Performance Manager collection.

Displaying Performance Manager Reports

This section includes the following topics:

You can view Performance Manager statistical data using preconfigured reports that are built on demand and displayed in a web browser. These reports provide summary information as well as detailed statistics that can be viewed for daily, weekly, monthly, or yearly results.

SUMMARY STEPS

1. Choose Performance > Reports to access Performance Manager reports from DCNM-SAN.
2. Click the Performance tab to view the Performance Manager reports.

DETAILED STEPS

Step 1 Choose Performance > Reports to access Performance Manager reports from DCNM-SAN.

This opens a web browser window showing the default DCNM-SAN web client event summary report.

Step 2 Click the Performance tab to view the Performance Manager reports.

Performance Manager begins reporting data ten minutes after the collection is started.

What to do next



Note DCNM-SAN Web Server must be running for reports to work.

Displaying Performance Summary

The Performance Summary page presents a dashboard display of the throughput and link utilization for hosts, ISLs, storage, and flows for the last 24-hour period. The summary provides a quick overview of the fabric's bandwidth consumption and highlights any hotspots.

The report includes network throughput pie charts and link utilization pie charts. Use the navigation tree on the left to show summary reports for monitored fabrics or VSANs. The summary displays charts for all hosts, storage elements, ISLs, and flows. Each pie chart shows the percent of entities (links, hosts, storage, ISLs, or flows) that measure throughput or link utilization on each of six predefined ranges. Move the mouse over a pie chart section to see how many entities exhibit that range of statistics. Double-click any pie chart to bring up a table of statistics for those hosts, storage elements, ISLs, or flows.

Displaying Performance Tables and Details Graphs

Click Host, Storage, ISL, or Flow to view traffic over the past day for all hosts, storage, ISLs, or flows respectively. A table lists all of the selected entities, showing transmit and receive traffic and errors and discards, if appropriate. The table can be sorted by any column heading. The table can also be filtered by day, week, month, or year. Tables for each category of statistics display average and peak throughput values and provide hot-links to more detailed information.

Clicking a link in any of the tables opens a details page that shows graphs for traffic by day, week, month, and year. If flows exist for that port, you can see which storage ports sent data. The details page also displays graphs for errors and discards if they are part of the statistics gathered and are not zero.

If you double-click a graph on a Detail report, it will launch the Cisco Traffic Analyzer for Fibre Channel, if configured. The aliases associated with hosts, storage devices, and VSANs in the fabric are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Displaying Performance of Host-Optimized Port Groups

You can monitor the performance of host-optimized port groups by selecting Performance > End Devices and selecting Port Groups from the Type drop-down list.

Displaying Performance Manager Events

Performance Manager events are viewed through DCNM-SAN Web Server. To view problems and events in DCNM-SAN Web Server, choose a fabric and then click the **Events** tab to see a summary or detailed report of the problems and events that have occurred in the selected fabric.

Generating Performance Manager Reports

Generating Top10 Reports in Performance Manager

You can generate historical Top10 reports that can be saved for later review. These reports list the entities from the data collection, with the most active entities appearing first. This is a static, one-time only report that generates averages and graphs of the data collection as a snapshot at the time the report is generated. These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the

other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated and are static. These are one-time reports that generate averages and graphs of the data collection as a snapshot at the time the report is generated.



Tip Name the reports with a timestamp so that you can easily find the report for a given day or week.

These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated.



Note Top10 reports require analyzing the existing data over an extended period of time and can take hours or more to generate on large fabrics.

Generating Top10 Reports Using Scripts

You can generate Top10 reports manually by issuing the following commands:



Note Cisco DCNM on Linux (RHEL), and Cisco DCNM for SAN OVA/ISO display the Top10 reports on **Web UI > Dashboard > Summary**.

- On UNIX, run the script:

```
"/<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>"
```

- On Windows, run the script:

```
"c:\Program Files\Cisco Systems\MDS 9000\bin\pm.bat display pm/pm.xml <output_directory>"
```

On UNIX, you can automate the generation of the Top10 reports on your DCNM-SAN Server host by adding the following cron entry to generate the reports once an hour:

```
0 * * * * /<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>
```

If your crontab does not run automatically or Java complains about an exception that is similar to the exception shown in the example below, you need to add “-Djava.awt.headless=true” to the JVMARGS command in /<user_directory>/cisco_mds9000/bin/pm.sh.

Example Java Exception

```
in thread "main" java.lang.InternalError Can't connect to X11 window server using '0.0' as the value of the DISPLAY variable.
```

Configuring Performance Manager for Use with Cisco Traffic Analyzer

Performance Manager works in conjunction with the Cisco Traffic Analyzer to allow you to monitor and manage the traffic on your fabric. Using Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

Step 1 Set up the Cisco Traffic Analyzer according to the instructions in the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

Step 2 Get the following three items of information:

- The IP address of the management workstation on which you are running Performance Manager and Cisco Traffic Analyzer.
- The path to the directory where Cisco Traffic Analyzer is installed.
- The port that is used by Cisco Traffic Analyzer (the default is 3000).

Step 3 Start the Cisco Traffic Analyzer.

- Choose **Performance > Traffic Analyzer > Open**.
- Enter the URL for the Cisco Traffic Analyzer, in the format:

Example:

```
http://<ip address>
>:<port number>
>
```

ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer

:port number is the port that is used by Cisco Traffic Analyzer (the default is :3000).

- Click **OK**.
- Choose **Performance > Traffic Analyzer > Start**.
- Enter the location of the Cisco Traffic Analyzer, in the format:

Example:

```
D:\<directory>
>\ntop.bat
```

D: is the drive letter for the disk drive where the Cisco Traffic Analyzer is installed.

directory is the directory containing the ntop.bat file.

- Click **OK**.

Step 4 Create the flows you want Performance Manager to monitor, using the Flow Configuration Wizard.

Step 5 Define the data collection you want Performance Manager to gather, using the Performance Manager Configuration Wizard.

- a) Choose the VSAN you want to collect information for or choose All VSANs.
- b) Check the types of items you want to collect information for (Hosts, ISLs, Storage Devices, and Flows).
- c) Enter the URL for the Cisco Traffic Analyzer in the format:

Example:

```
http://<ip address>/<directory>
```

where:

ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer, and directory is the path to the directory where the Cisco Traffic Analyzer is installed.

- d) Click **Next**.
- e) Review the data collection on this and the next section to make sure this is the data you want to collect.
- f) Click **Finish** to begin collecting data.

Note Data is not collected for JBOD or for virtual ports. If you change the data collection configuration parameters during a data collection, you must stop and restart the collection process for your changes to take effect.

Step 6 Choose **Performance > Reports** to generate a report. Performance Manager Web Server must be running. You see Web Services; click **Custom** then select a report template.

Note It takes at least five minutes to start collecting data for a report. Do not attempt to generate a report in Performance Manager during the first five minutes of collection.

Step 7 Click **Cisco Traffic Analyzer** at the top of the Host or Storage detail pages to view the Cisco Traffic Analyzer information, or choose **Performance > Traffic Analyzer > Open**. The Cisco Traffic Analyzer page will not open unless ntop has been started already.

Note For information on capturing a SPAN session and starting a Cisco Traffic Analyzer session to view it, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

Note For information on viewing and interpreting your Performance Manager data. For information on viewing and interpreting your Cisco Traffic Analyzer data, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

What to do next

For performance drill-down, DCNM-SAN Server can launch the Cisco Traffic Analyzer in-context from the Performance Manager graphs. The aliases associated with hosts, storage devices, and VSANs are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Exporting Data Collections

This section includes the following topics:

Exporting Data Collections to XML Files

The RRD files used by Performance Manager can be exported to a freeware tool called rrdtool. The rrd files are located in pm/db on the DCNM-SAN Server. To export the collection to an XML file, enter the following command at the operating system command-line prompt:

```
/bin/pm.bat xport xxx yyy
```

In this command, xxx is the RRD file and yyy is the XML file that is generated. This XML file is in a format that rrdtool is capable of reading with the command:

```
rrdtool restore filename.xml filename.rrd
```

You can import an XML file with the command:

```
bin/pm.bat pm restore <xmlFile> <rrdFile>
```

This reads the XML export format that rrdtool is capable of writing with the command:

```
rrdtool xport filename.xml filename.rrd.
```

The pm xport and pm restore commands can be found on your DCNM-SAN Server at bin\PM.bat for Windows platforms or bin/PM.sh on UNIX platforms. For more information on the rrdtool, refer to the following website: <http://www.rrdtool.org>.

Exporting Data Collections in Readable Format

You can export the RRD files used by Performance Manager to a freeware tool called rrdtool and export the collection to an XML file. Cisco MDS SAN-OS Release 2.1(1a) introduces the inability to export data collections in comma-separated format (CSV). This format can be imported to various tools, including Microsoft Excel. You can export these readable data collections either from the DCNM-SAN Web Services menus or in batch mode from the command line on Windows or UNIX. Using DCNM-SAN Web Services, you can export one file. Using batch mode, you can export all collections in the pm.xml file.



Note DCNM-SAN Web Server must be running for this to work.

You can export data collections to Microsoft Excel using DCNM-SAN Web Server.

SUMMARY STEPS

1. Click the Performance tab on the main page.
2. Click the **Flows** sub-tab.
3. Right-click the name of the entity you want to export and select **Export to Microsoft Excel**.

DETAILED STEPS

-
- Step 1** Click the Performance tab on the main page.
You see the overview table.
- Step 2** Click the **Flows** sub-tab.
- Step 3** Right-click the name of the entity you want to export and select **Export to Microsoft Excel**.
You see the Excel chart for that entity in a pop-up window.
-

Exporting Data Collections in Readable Format

You can export data collections using command-line batch mode.

SUMMARY STEPS

1. Go to the installation directory on your workstation and then go to the bin directory.
2. On Windows, enter `.\pm.bat export C:\Program Files\Cisco Systems\MDS 9000\pm\pm.xml <export directory>`. This creates the csv file (export.csv) in the export directory on your workstation.
3. On UNIX, enter `./pm.sh export /usr/local/cisco_mds9000/pm/pm.xml <export directory>`. This creates the csv file (export.csv) in the export directory on your workstation.

DETAILED STEPS

-
- Step 1** Go to the installation directory on your workstation and then go to the bin directory.
- Step 2** On Windows, enter `.\pm.bat export C:\Program Files\Cisco Systems\MDS 9000\pm\pm.xml <export directory>`. This creates the csv file (export.csv) in the export directory on your workstation.
- Step 3** On UNIX, enter `./pm.sh export /usr/local/cisco_mds9000/pm/pm.xml <export directory>`. This creates the csv file (export.csv) in the export directory on your workstation.
-

What to do next

When you open this exported file in Microsoft Excel, the following information displays:

- Title of the entity you exported and the address of the switch the information came from.
- The maximum speed seen on the link to or from this entity.
- The VSAN ID and maximum speed.
- The timestamp, followed by the receive and transmit data rates in bytes per second.

Analyzing SAN Health

The SAN Health Advisor tool is a utility that used to monitor the performance and collect the statistics. You can perform the following tasks with this tool:

- Run Performance Monitor to collect I/O statistics
- Collect fabric inventory (switches and other devices)
- Create a graphical layout of fabric topology
- Create reports of error conditions and statistical data

You can install this tool at any SAN environment to collect I/O statistics for the specified time (usually 24 hours), generate health reports and automatically send reports to the designated system administrator for review at regular intervals.

When you start SAN Health Advisor tool, it runs in wizard mode, and prompts for inputs such as seed switch credentials, IP address of the server to which the data to be sent and all the necessary information for the software setup. As soon as the fabric is discovered, the tool starts capturing performance data, I/O statistics and error conditions.

The reports generated from the collection is stored in the \$INSTALLDIR/dcm/fm/reports directory. These reports are automatically sent to the designated SAN administrator for review. In a situation where the tool fails to collect the data, it generates a report with an error message or exception. After sending the reports the tool automatically uninstalls itself and terminates all the processes that it established on the host machine.

The report that SAN Health Advisor tool generates will have the following details:

- Events
- System messages
- Analysis of connectivity
- Zone discrepancy
- System configuration
- Interface status
- Domain information
- Security settings

Installing the SAN Health Advisor Tool

SAN Health Advisor tool can be installed and run on Windows, UNIX, and Solaris platforms. Install the package that contains the .jar file with JRE version 6.0.



Note The SAN Health tool is not installed by default when you install DCNM-SAN software.

-
- Step 1** Double-click the San Health Advisor tool installer.
You see the San Health Advisor tool Installer window.
- Step 2** Select an installation folder on your workstation for SAN Health Advisor.
On Windows, the default location is C:\Program Files\Cisco Systems\.
- Step 3** Click Install to start the installation.
You will see the installation progressing.
You will see the Fabric Options dialog box.
- Step 4** In the Seed Switch text box, enter the IP address of the seed switch.
- Step 5** Enter the user name and password for the switch.
- Step 6** Select the authentication privacy option from the Auth-Privacy drop-down list box.
- Step 7** Click the Performance Collection check box to enable the process to run for 24 hours.
- Step 8** Click Collect to start gathering performance information.
If you want to stop gathering information in the middle of the process, click Cancel.
- Step 9** Click Uninstall to remove the SAN Health Advisor software.
-

Monitoring the LAN Switch Performance Counters

DCNM allows you to monitor LAN switch performance counters. The following counters can be monitored:

- Performance monitoring of interfaces (RX/TX traffic statistics, errors/discards, average/peak statistics etc.)
- Monitor VPC member Rx/Tx counters.
- Monitor CPU/Memory statistics.
- Monitor switch traffic.
- Monitor Health Scores.
- Monitor Events.

