

ENM System Monitor User Guide

User Guide

Copyright

© Ericsson AB 2017-2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document [Trademark Information](#).



Contents

1	Introduction	1
2	ESM Overview	2
3	Access ESM	3
3.1	Change Default Password for ESM Users	4
4	Navigate ESM User Interface	6
4.1	Configure the Dashboard	6
4.2	Customize Views	7
4.3	Alerted or Unavailable Resources	8
5	Inventory	9
6	Access ESM Operating System Metrics	12
6.1	ESM Operating System Metrics	14
7	View ESM Hardware Metrics	15
7.1	ESM Hardware Metrics	17
8	ENM Metrics	18
8.1	ESM Application Metrics	18
8.2	Description of ESM Metrics	22
8.3	Access ESM Common Metrics	32
8.4	Access VM Availability Metrics	36
8.5	Access VM Group Availability Metrics	36
9	View Resource Metrics	38
10	Enabling and Disabling Metrics of a Specific Resource	42
11	ENM System Monitor Alerts	44
11.1	View Alert Information	46
11.2	Create FM Alert Notifications	48
11.3	Create Internal Alerts	58
11.4	Update an Existing Alert	62
11.5	Delete Alert Definition Template of a Given Resource	63
12	View Default ESM Alert Thresholds	65



12.1	View File System Alert Thresholds	65
12.2	View Linux Alert Thresholds	68
12.3	View Snapshots Status Alert Thresholds	70
12.4	View VM Group Availability Alert Thresholds	72
12.5	Edit Conditions	74
13	View Alerts for EMC Clariion or VNX Storage	76
13.1	Default Threshold for ENM Storage	77
13.2	ESM EMC Metrics	78
	Reference List	79



1 Introduction

ENM System Monitor (ESM) monitors the performance of servers and applications, raises alarms on breach of predefined thresholds. It provides a web interface to control and display the data it handles.

Purpose

This document describes how to use ESM User Interface.

Target groups

The intended target groups for this document are as follows:

- Non-Administrative Users

Requirements

The user is assumed to have the following:

- Knowledge of how to access the ENM homepage.
- Appropriate ID, account, and permissions.

The user is using one of the following web browsers:

- Chrome stable latest (ENM is verified on Chrome 47).
- Firefox ESR latest (ENM is verified on Firefox 38.4.0, 42).



2 ESM Overview

ENM System Monitor (ESM) consists of a single-instance server and multiple agents. The agents are installed on various platforms including Management Server (MS) to be monitored.

The agents transmit information to the server where it is displayed on a portal, which the user views using a supported web browser. The information displayed is used to determine if the ENM servers being monitored are operating correctly.

The key components of ESM are:

- RHQ Server
- RHQ Agent(s)
- A supported database
- JMX enabled resources to monitor.

This section contains the routine operation and maintenance tasks related to the System Monitoring application.

ENM System Monitor performs the following functions:

- Monitoring of hardware metrics for all server platforms
- Monitoring of operating system metrics for all server platforms
- Monitoring of metrics that are exposed by ENM applications
- Alerting of any breach of a configured threshold on a metric
- Forwarding of alerts as a stateful alarm to ENM fault management
- Near-realtime and historical viewing of metrics

ENM System Monitor provides a web-based application for performing management actions.

A customizable portal offers critical information quickly to the right audiences.



3 Access ESM

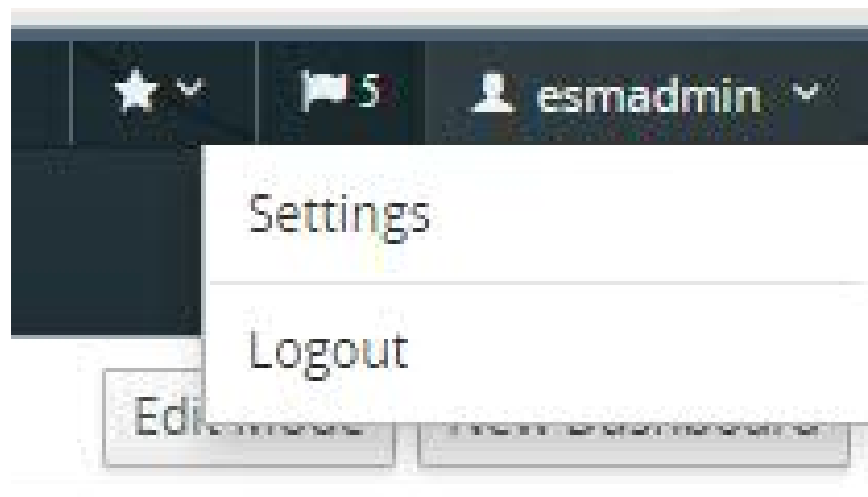
This task describes how to access ESM.

Steps

1. Log on to ENM launcher page as an administrator or as a user with System_Monitor role.
2. Click the **ENM System Monitor** link.
3. Enter the username and password supplied by local Ericsson support.
4. Click **Log in**.
5. It is recommended to change the default password after the first login. See section [Change Default Password for ESM Users](#) on page 4 for more details.

Note: If the web portal is inactive for longer than the maximum idle time period, the session is closed automatically.

To log out, select **Logout** from the top-right corner of any page.



Results

ESM Dashboard is launched.



— RELATED INFORMATION —

[3.1 Change Default Password for ESM Users on page 4](#)

[Reference List on page 79](#)

3.1 Change Default Password for ESM Users

ESM user is provided with the default password by local Ericsson support. The default password of ESM user is to be changed when the user logs in for the first time.

Prerequisites

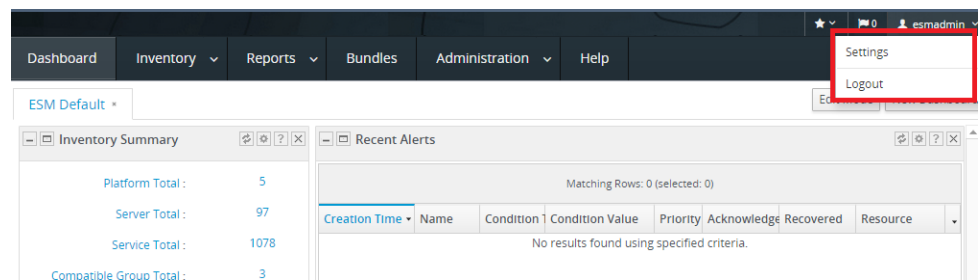
User is logged on to ENM launcher page as administrator or as user with System_Monitor role.

Stop!

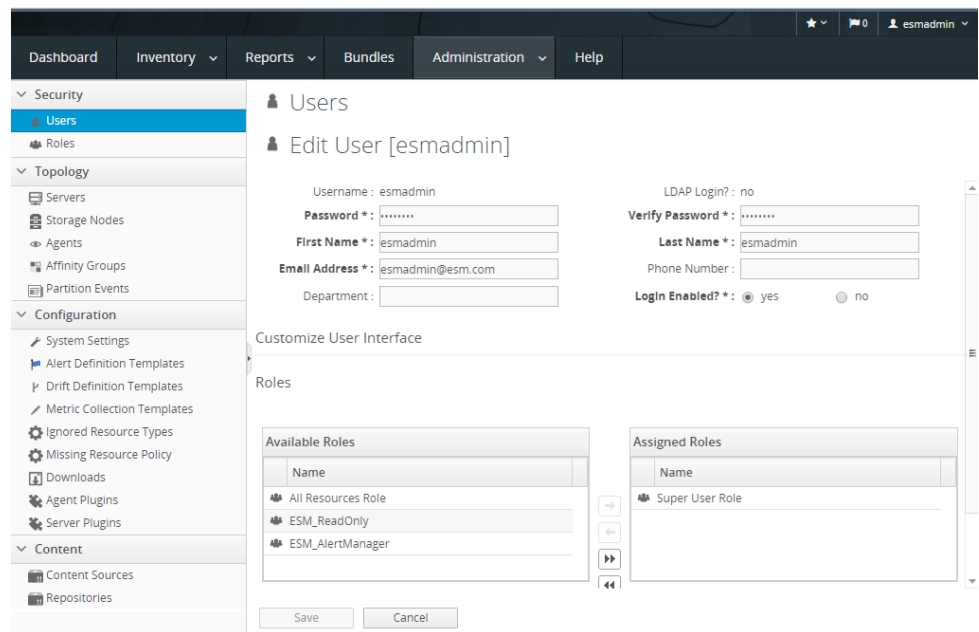
Do not change the default password of **rhqadmin** username, which is internally used to configure the RHQ server and do scheduled tasks. Changing the default password of the username **rhqadmin** results in failure of the rpm installations and causes the upgrade or rollback to fail.

Steps

1. Log on to ENM launcher page as administrator or as user with System_Monitor role.
2. Click **ENM System Monitor** link.
3. Log on to the ESM using the username and password that are provided in section *User Management for ENM System Monitor* of [ENM Identity and Access Management System Administrator Guide](#).
4. Click **Log in**.
5. Navigate to the user at the top right section and click it.



6. Click **Settings**.



7. Enter the new password in the **Password** and **Verify Password** fields.

8. Click **Save**.

9. Change default passwords after first logon.

Results

Default password of ESM is changed.



4 Navigate ESM User Interface

ESM user interface provides access to view all resources and event information. The ESM interface is available to all ESM defined users.

- Note:**
- ESM uses the 3PP tool. Check out the following site for help information on using it: <https://docs.jboss.org/author/display/RHQ/Release+Notes+4.13>.
 - ESM GUI fails to open if the system date or time is incorrect, which is a known 3PP limitation.

— RELATED INFORMATION —

[4.1 Configure the Dashboard on page 6](#)

[4.2 Customize Views on page 7](#)

[4.3 Alerted or Unavailable Resources on page 8](#)

4.1 Configure the Dashboard

Dashboard contains multiple views, each of which presents a summary view of events and resources.

Dashboard contains the following views:

- Recent Alerts
- Alerted or Unavailable Resources
- Recent Operations
- Inventory Summary

- Note:**
- Some alerts may be duplicated in **Recent Alert** view.
 - **Recent Alerts** view cannot be sorted..

Each of the views presents a summary view of events and resources.

Dashboard can be tailored based on individual user and customized by reorganizing the views and filtering the data shown.



The screenshot shows the ESM web console interface with a top navigation bar containing 'Dashboard', 'Inventory', 'Reports', 'Bundles', 'Administration', and 'Help'. A notification indicates 'Saved dashboard ESM Default to server'. The main content area is titled 'ESM Default' and contains several portlets:

- Inventory Summary:** A summary of system metrics including Platform Total (5), Server Total (99), Service Total (1078), Compatible Group Total (3), Mixed Group Total (1), Group Definition Total (6), and Average Metrics per Minute (381).
- Recent Alerts:** A table showing alert details. One alert is visible: '1/23/17 3:19 PM Linux - Idle - Clear' with a condition value of 22.6% and resource 'cloud-ms-1'.
- Platform Utilization:** A table showing resource utilization for 'cloud-ms-1' and 'esmc' across various metrics like CPU, Mem, and Swap.
- Alerted or Unavailable Resources:** A table listing resources and their alert status. Resources include 'cloud-ms-1', 'esmon', and 'cmp'.

Steps


1. Click **New Dashboard** at the top-right of the ESM web console to create a new **Dashboard** tab.
2. Click **X** located in the **Dashboard** tab to delete a dashboard.
3. To automatically refresh your dashboard to periodically pick up new data, use the **Refresh Interval** drop-down menu.
4. Disable automatic refresh by turning off this feature.

4.2 Customize Views

Each dashboard can have any number of views.

The limitation to the number of views you can have is limited to your monitor's screen size.

Steps

1. Use the **Add Portlet** drop down menu to pick the view you want to add.
2. Some views support further customization through their configure icon  found in the top-right corner of the view's title bar.



3. You can move the views around the dashboard by clicking and dragging the view's title bar.
4. To remove a view from a dashboard, click X located in the top-right corner of the view's title bar.

4.3 Alerted or Unavailable Resources

This portlet shows the unavailable resources or the alerts for the resources that have been raised on.

Unavailable resources include file systems, CPU, and any services on a platform. If any of the resources are configured to be highly available, which means if it is deployed on a different service groups (VMs) either in active-active or active-passive mode, this section shows only the resources which went down.

ESM cannot detect if a resource is going down in one platform, the same resource is available on another platform. ESM treats each resource independently.

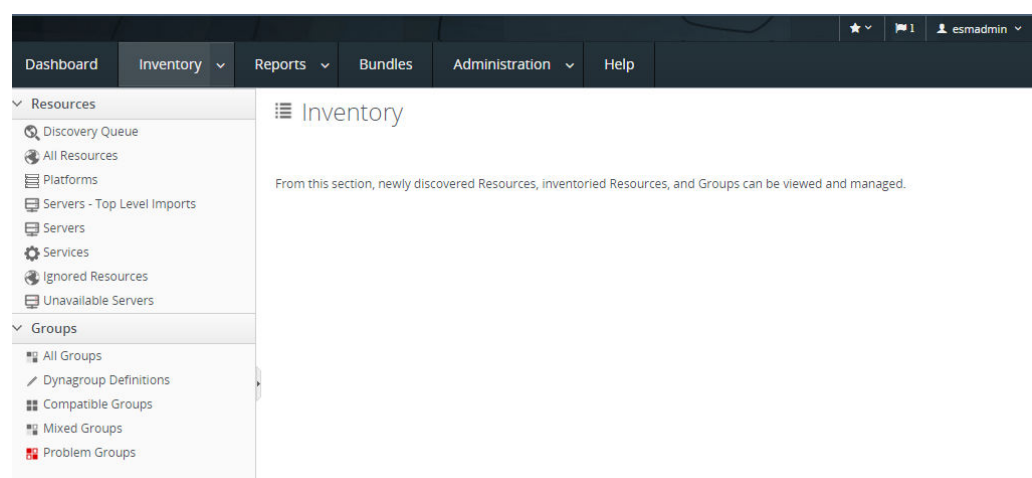
Alerted or Unavailable Resources			
Total: 20			
Resource	Ancestry	Alerts	Availability
/ericsson/elasticsearch	ieatrcrb6459	8	⊗
/ericsson/enm/dumps	ieatrcrb6445	2	⊗
/ericsson/enm/dumps	ieatrcrb6459	2	⊗
/ericsson/enm/dumps	ieatrcrb6464	2	⊗
/ericsson/enm/dumps	ieatrcrb5227	2	⊗
/ericsson/enm/dumps	ieatrcrb6454	2	⊗
/ericsson/enm/dumps	ieatrcrb6458	2	⊗
/ericsson/enm/dumps	ieatrcrb6453	2	⊗
/ericsson/enm/dumps	ieatrcrb6463	2	⊗
/ericsson/enm/dumps	ieatrcrb6461	2	⊗
/ericsson/enm/dumps	ieatrcrb6482	2	⊗
/ericsson/versant_bar/backup/mount_snap	ieatrcrb6464	1	⊗
/ericsson/versant_bar/backup/mount_snap	ieatrcrb6445	1	⊗
EAP (1327.0.0.1:6990) RHQ Server	esmon	0	⊗
/ENM_BACKUP/root_lvmt/home	ieatims337	0	⊗
/ENM_BACKUP/root_lvmt/root	ieatims337	0	⊗



5 Inventory

The Inventory page provides access to all resources monitored by the application.

The page can be accessed by selecting the **Inventory** tab on the top navigational bar.



The main section of the Inventory page is the **Resources** list. All monitored systems can be found under its various subsections.

Discovery Queue

Only system administrators have access to the Discovery Queue.

All Resources

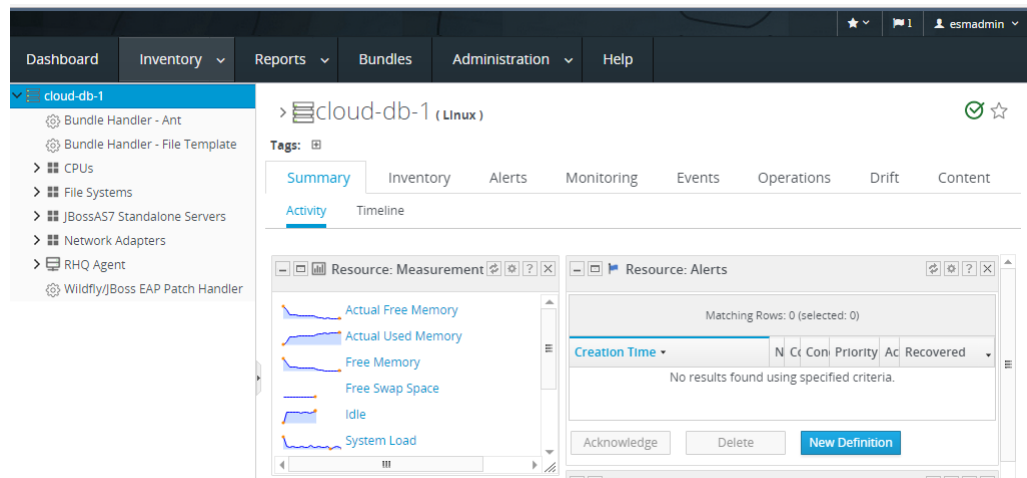
All Resources page displays all resources monitored by the system across all platforms.

Non-administrator users can use this list to search for and view metric data of any resource by selecting its name from the list.

Platforms

Platforms page lists all monitored systems at the operating system level.

Every platform on the list can be selected to view its specific metrics.



Note: Availability is not updated automatically, a browser refresh is required to get the updated status.

Servers - Top Level Imports

Servers page lists all monitored resources with server functionality, but it does not include resources under them.

Every server on the list can be selected to view its specific metrics.

Servers

This page lists all monitored resources with server functionality, including their child servers.

Every resource on the list can be selected to view its specific metrics.

Service

Service page lists all resources detected on Servers (for example, a JMS Queue on a JBoss AS server).

Ignored Resources

Ignored Resources page lists all resources that are explicitly ignored by the system.

Unavailable Servers

Unavailable Servers page lists all resources that were detected but can not be contacted to collect new metrics.



Groups

Groups are not supported in ESM.



6 Access ESM Operating System Metrics

ESM collects the operating system metrics. These metrics are visible to all the users of ESM and no specific permissions are required to view them.

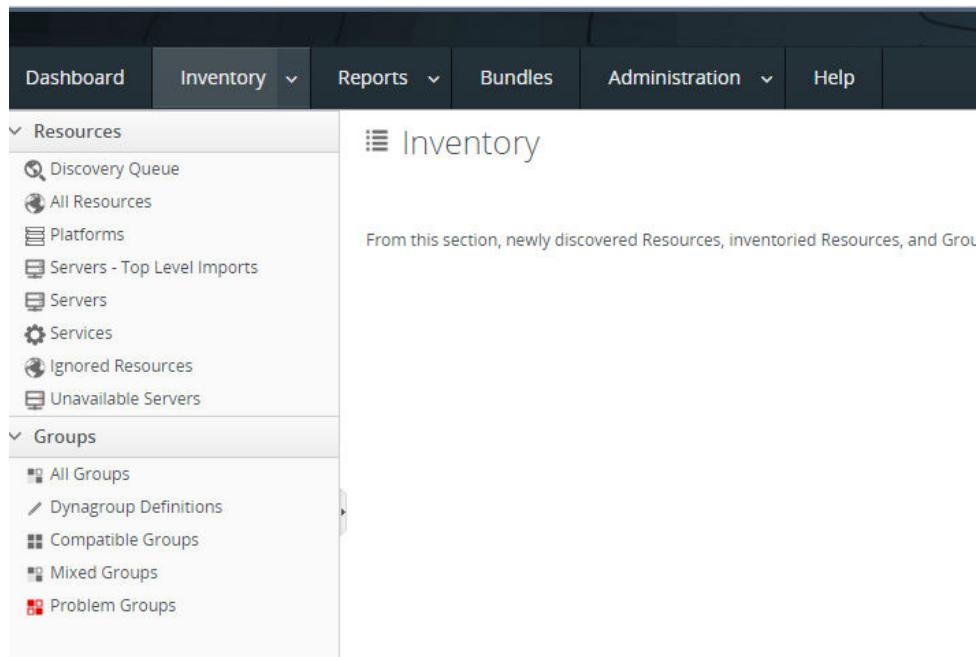
The metrics are collected on a per-minute basis.

Prerequisites

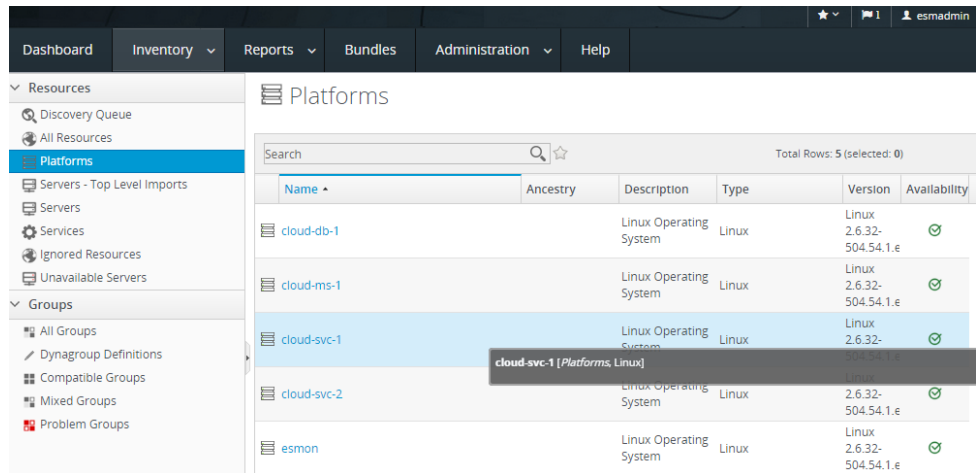
The user is logged on to ESM.

Steps

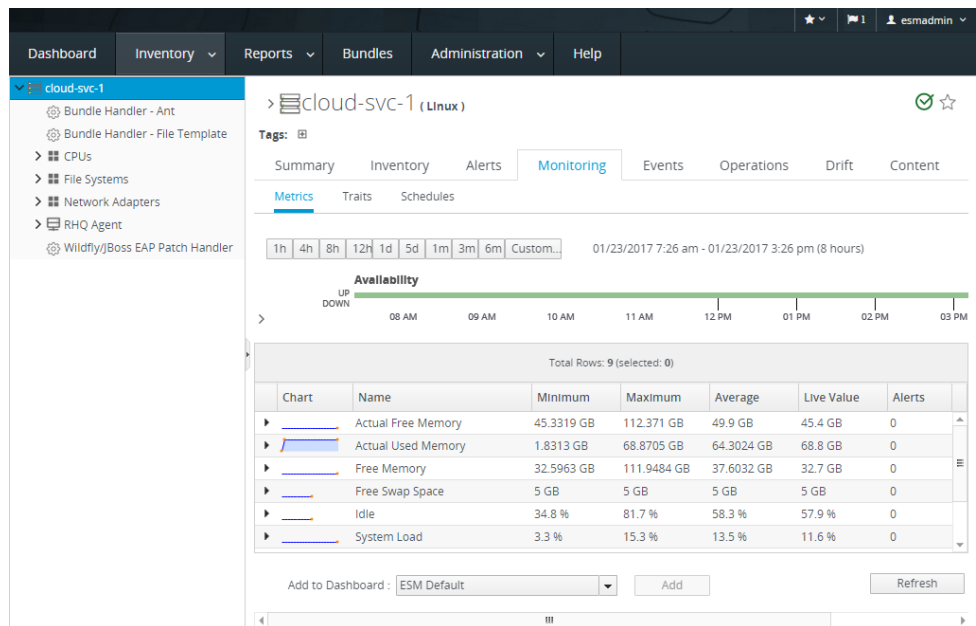
1. Click **Inventory**.



2. Click **Platforms**.
3. Select any platform from the list.



4. Click **Monitoring > Metrics** to view all metrics collected for the specified platform.



Results

The user is able to access Operating System Metrics that are collected by ESM.

— RELATED INFORMATION —

[6.1 ESM Operating System Metrics on page 14](#)



6.1 ESM Operating System Metrics

The following table contains the list of Operating System Metrics that are collected by ESM.

Table 1 ESM Operating System Metrics

S.No	Metric Name	Description
1	Actual Free Memory	The actual total free system memory (includes unallocated memory as well as available buffer and measurement cache memory)
2	Actual Used Memory	The actual total used system memory (includes buffer and cache memory)
3	Free Memory	The total free system memory (does not include buffer or cache memory)
4	Free Swap Space	The total free system swap
5	System Load	Percentage of all CPU's running in system mode.
6	Used Memory	The total used system memory (does not include buffer or cache memory)
7	Used Swap Space	The total used system swap
8	Used Load	Percentage of all CPU's running in User mode.



7 View ESM Hardware Metrics

ESM collects hardware metrics. All CPU, file system, and network adapter metrics are available under Hardware Metrics.

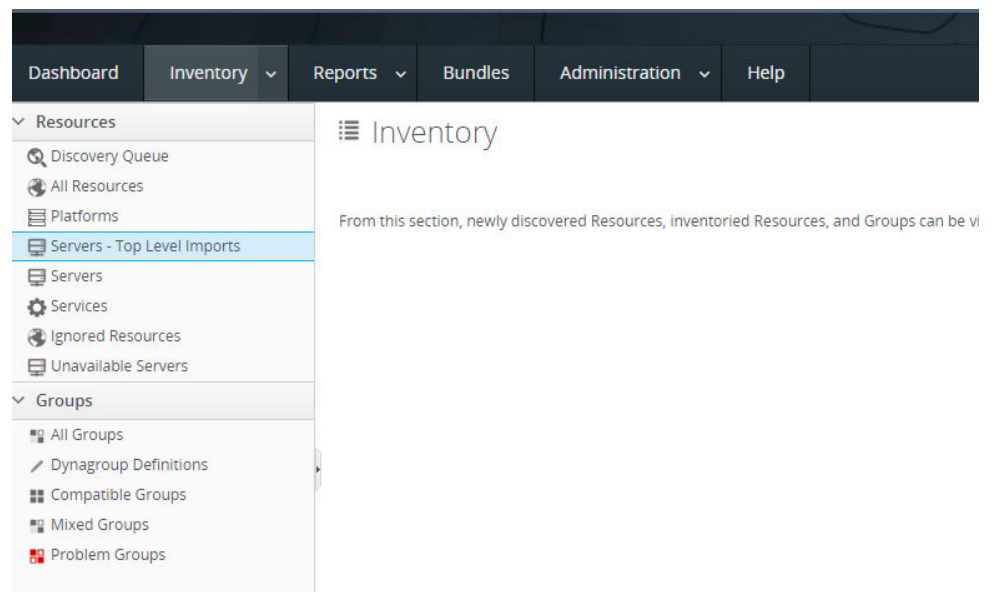
The metrics are collected per-minute basis.

Prerequisites

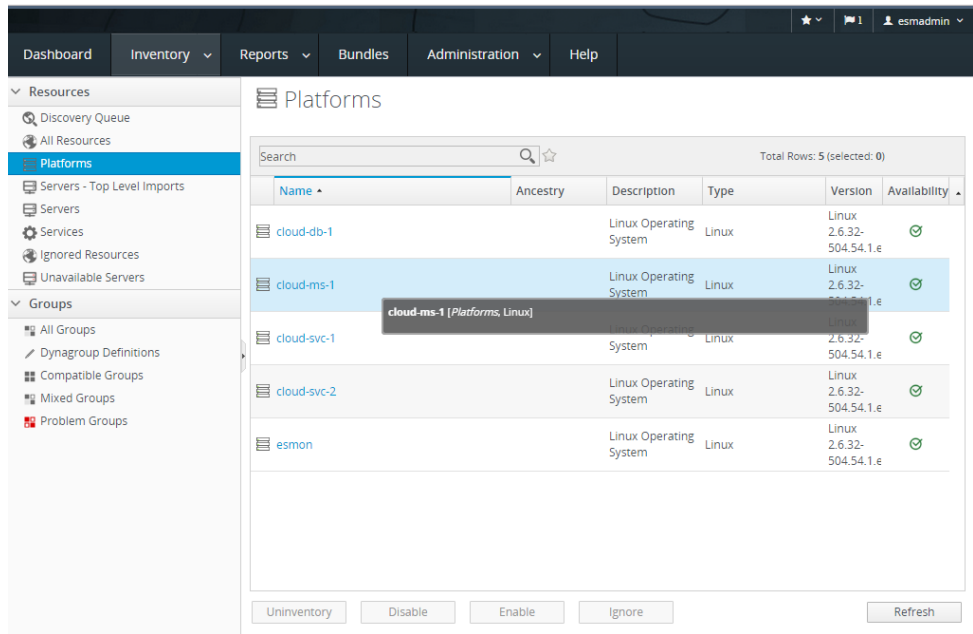
The user is logged on to ESM. These metrics are visible to all the users of ESM and no specific permissions are required to view them.

Steps

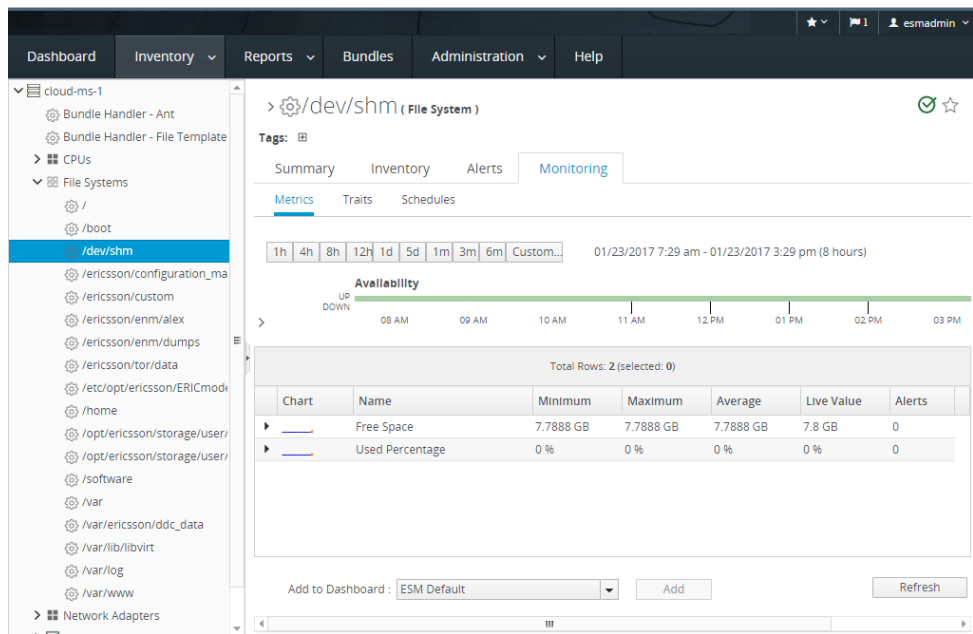
1. Log on to ESM.
2. Click **Inventory**.



3. Click **Platforms**.
4. Select any platform from the list.



- 5. Select **CPU > File System > Network Adapter**, and click the **Monitoring** tab to view the hardware related metrics to that platform.



Results

The user should be able to view the hardware metrics that are collected by ESM.



— RELATED INFORMATION —

[7.1 ESM Hardware Metrics on page 17](#)

7.1 ESM Hardware Metrics

The following tables contain the list of hardware metrics that are collected by ESM.

Table 2 CPU Metrics

S.No	Metric Name	Description
1	System Load	Percentage of this CPU running in system mode
2	User Load	Percentage of this CPU running in user mode
3	Wait Load	Percentage of this CPU waiting on I/O

Table 3 File System Metrics

S.No	Metric Name	Description
1	Free Space	The total free bytes on file system
2	Used Percentage	Percentage of disk used

Table 4 Network Adapter Metrics

S.No	Metric Name	Description
1	Bytes received per minute	The total number of bytes received across this network interface since it started.
2	Bytes transmitted per minute	The total number of bytes transmitted across this network interface since it started.



8 ENM Metrics

This section describes the application metrics and common metrics that are collected by ESM. ESM collects Application Metrics for all the applications that expose their metrics. These metrics are collected per-minute basis.

The metrics are visible to all the users of ESM, and no specific permissions are required to view them.

— RELATED INFORMATION —

[8.1 ESM Application Metrics on page 18](#)

[8.3 Access ESM Common Metrics on page 32](#)

[8.4 Access VM Availability Metrics on page 36](#)

[8.5 Access VM Group Availability Metrics on page 36](#)

8.1 ESM Application Metrics

This section describes the Application Metrics that are collected by ESM. ESM collects Application Metrics for all applications that expose their metrics. These metrics are collected per-minute basis. These Application Metrics are visible to all the users of ESM and no specific permissions are required to view them.

Prerequisites

The user is logged on to ESM.

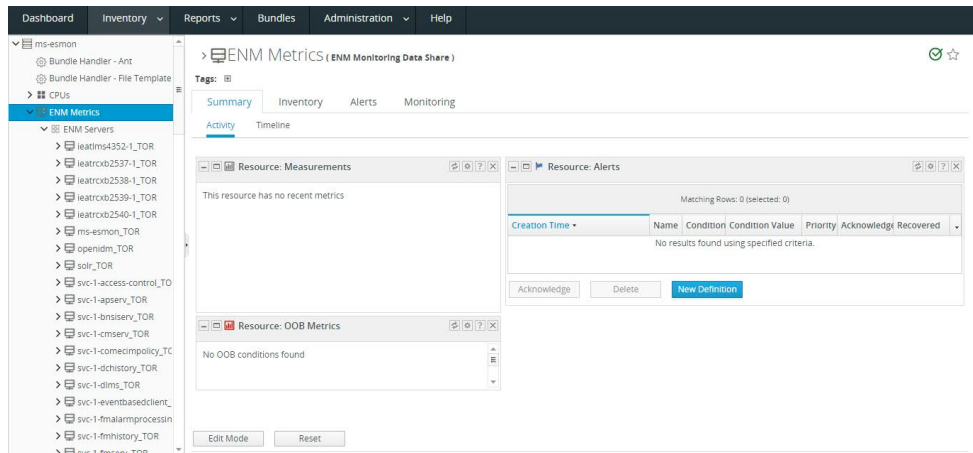
Steps

1. Click **Inventory**.

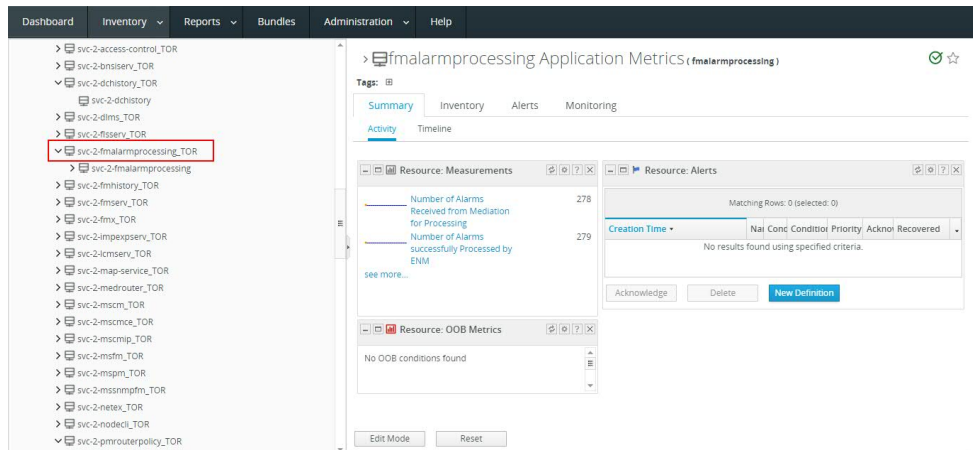


2. Click **Platforms**.
3. Select esmon platform.
4. Click **ENM Metrics**.

5. Click **ENM Servers**.

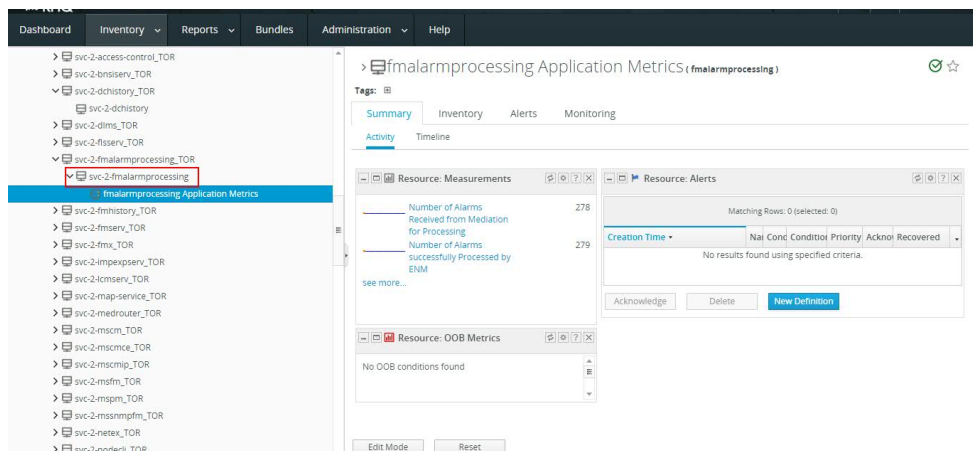


6. Click any Virtual Machine (VM).



7. Click the immediate child resource of the VM.

That is the name of the VM.



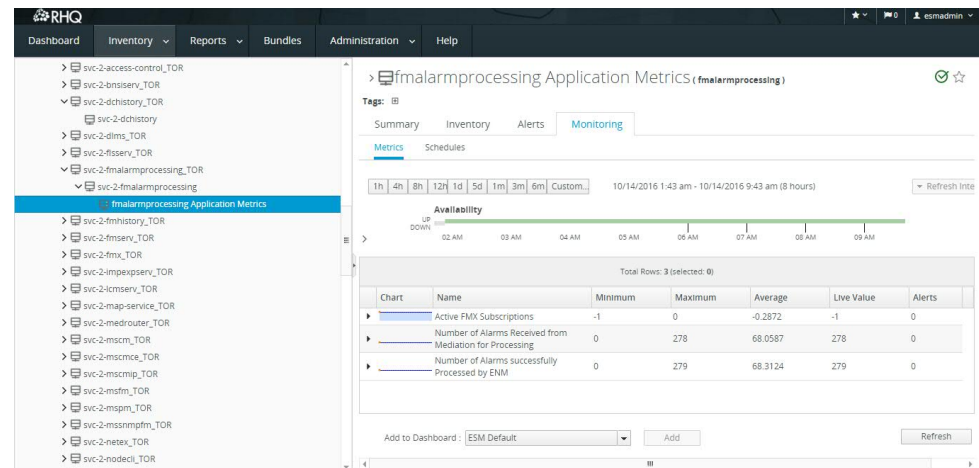
8. Click its immediate child resource.



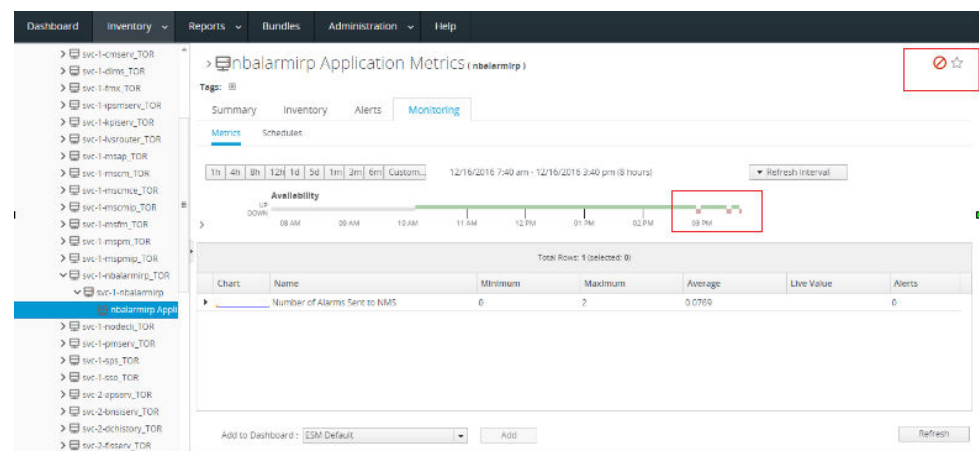
Example

fmalarmprocessing Application Metrics

- Click **Monitoring > Metrics** to view all the metrics that are collected.



- Unavailability of instrumentation data for more than five minutes of particular application is shown in red.



Results

The user is able to access Application Metrics that are collected by ESM.

Note: For more information on FM application metrics, refer to the [ENM Monitoring System Administrator Guide](#).

For more information on AMOS application metrics, refer to the [ENM Configuration System Administrator Guide](#).

For more information on PMIC application metrics, refer to the [ENM Performance Management System Administrator Guide](#).



8.2 Description of ESM Metrics

Table 5 AMOS

S.No	Metrics Name	Description
1	cpuUsed	Current CPU Usage of a virtual machine.
2	memoryUsed	Current Memory Usage of a virtual machine.
3	sessions	Current number of AMOS Sessions running in the virtual machine.

Table 6 Domain Proxy

S.No	Metrics Name	Description
1	numberOfActiveCellsCount	Number of active cells managed by domain proxy.
2	numberOfFailedCbsdRegistrationsIncremental	Number of failed CBSD registrations.
3	numberOfFailedConnectionAttemptsWithSasIncremental	Number of failed http/tls connections counter for SAS.
4	numberOfInactiveCellsCount	Number of inactive cells managed by domain proxy.
5	numberOfMaintainedGrantsCount	Number of authorized grants maintained by domain proxy.
6	numberOfRegisteredCbsdsCount	Number of registered CBSDs.
7	numberOfRelinquishedGrantsIncremental	Number of grants relinquished by domain proxy.
8	numberOfRevokedGrantsIncremental	Number of grants revoked. That is terminated, expired or auto de-registration from SAS.
9	numberOfSuspendedGrantsIncremental	Number of grants suspended by a SAS.



S.No	Metrics Name	Description
10	numberOfTerminatedGrantsIncremental	Number of grants terminated by a SAS.
11	numberOfValidGrantsCount	Number of valid grants.
DEPRECATED METRICS		
1	numberOfActiveCellsCount::domain-proxy-service	Number of active cells managed by domain proxy.
2	numberOfFailedCbsdRegistrationsIncremental::domain-proxy-service_trendsUp	Number of failed CBSD registrations.
3	numberOfFailedConnectionAttemptsWithSasIncremental::domain-proxy-service_trendsUp	Number of failed http/tls connections counter for SAS.
4	numberOfInactiveCellsCount::domain-proxy-service	Number of inactive cells managed by domain proxy.
5	numberOfMaintainedGrantsCount::domain-proxy-service	Number of authorized grants maintained by domain proxy.

Table 7 Fault Management

S.No	Metrics Name	Description
1	activeSubscriptionsCount	Active FMX subscriptions.
2	alarmCountReceivedByAPS	Number of alarms received by Fault Management.
3	alarmProcessedByAPS	Number of alarms processed by Fault Management.



Table 8 Performance Management

S.No	Metrics Name	Description
1	combinedNumberOfFilesCollected	Combined ROPs: number of files collected.
2	combinedNumberOfFilesFailed	Combined ROPs: number of files failed.
3	combinedNumberOfStoredBytes	Combined ROPs: number of stored bytes.
4	combinedNumberOfTransferredBytes	Combined ROPs: number of transferred bytes.
5	oneMinuteRopNumberOfFilesCollected	1 minute ROP: number of files collected.
6	oneMinuteRopNumberOfFilesFailed	1 minute ROP: number of files failed.
7	oneMinuteRopNumberOfStoredBytes	1 minute ROP: number of stored bytes.
8	oneMinuteRopNumberOfTransferredBytes	1 minute ROP: number of transferred bytes.
9	fiveMinutesRopNumberOfFilesCollected	5 minutes ROP: number of files collected.
10	fiveMinutesRopNumberOfFilesFailed	5 minutes ROP: number of files failed.
11	fiveMinutesRopNumberOfStoredBytes	5 minutes ROP: number of stored bytes.
12	fiveMinutesRopNumberOfTransferredBytes	5 minutes ROP: number of transferred bytes.
13	fifteenMinutesRopNumberOfFilesCollected	15 minutes ROP: number of files collected.
14	fifteenMinutesRopNumberOfFilesFailed	15 minutes ROP: number of files failed.
15	fifteenMinutesRopNumberOfStoredBytes	15 minutes ROP: number of stored bytes.
16	fifteenMinutesRopNumberOfTransferredBytes	15 minutes ROP: number of transferred bytes.
17	thirtyMinutesRopNumberOfFilesCollected	30 minutes ROP: number of files collected.



S.No	Metrics Name	Description
18	thirtyMinutesRopNumberOfFilesFailed	30 minutes ROP: number of files failed.
19	thirtyMinutesRopNumberOfStoredBytes	30 minutes ROP: number of stored bytes.
20	thirtyMinutesRopNumberOfTransferredBytes	30 minutes ROP: number of transferred bytes.
21	oneHourRopNumberOfFilesCollected	1 hour ROP: number of files collected.
22	oneHourRopNumberOfFilesFailed	1 hour ROP: number of files failed.
23	oneHourRopNumberOfStoredBytes	1 hour ROP: number of stored bytes.
24	oneHourRopNumberOfTransferredBytes	1 hour ROP: number of transferred bytes.
25	twelveHourRopNumberOfFilesCollected	12 hours ROP: number of files collected.
26	twelveHourRopNumberOfFilesFailed	12 hours ROP: number of files failed.
27	twelveHourRopNumberOfStoredBytes	12 hours ROP: number of stored bytes.
28	twelveHourRopNumberOfTransferredBytes	12 hours ROP: number of transferred bytes.
29	twentyFourRopNumberOfFilesCollected	24 minutes ROP: number of files collected.
30	twentyFourRopNumberOfFilesFailed	24 minutes ROP: number of files failed.
31	twentyFourRopNumberOfStoredBytes	24 hours ROP: number of stored bytes.
32	twentyFourRopNumberOfTransferredBytes	24 hours ROP: number of transferred bytes.

Table 9 Scripting

S.No	Metrics Name	Description
1	cpuUsed	Current CPU usage of a virtual machine.



S.No	Metrics Name	Description
2	memoryUsed	Current memory usage of a virtual machine.
3	sessions	Current number of AMOS sessions running in the virtual machine.

Table 10 Configuration Management

S.No	Metrics Name	Description
1	numberOfSuccessfulSubscriptions	Number of successful CM Subscriptions.
2	numberOfSupervisedNodes	Number of CM supervised nodes.
3	numberOfSynchronizedNodes	Number of synchronized nodes.
4	numberOfSuccessfulSubscriptions::APG-CM-ROUTER-POLICY	Number of successful CM subscriptions.
5	numberOfSupervisedNodes::APG-CM-ROUTER-POLICY	Number of CM supervised nodes.
6	numberOfSynchronizedNodes::APG-CM-ROUTER-POLICY	Number of synchronized nodes.
7	numberOfSuccessfulSubscriptions::SNMP-CM-ROUTER-POLICY	Number of successful CM subscriptions.
8	numberOfSupervisedNodes::SNMP-CM-ROUTER-POLICY	Number of CM supervised nodes.
9	numberOfSynchronizedNodes::SNMP-CM-ROUTER-POLICY	Number of synchronized nodes.
10	numberOfSuccessfulSubscriptions::cm-router-policy	Number of successful CPP CM subscriptions.
11	numberOfSupervisedNodes::cm-router-policy	Number of CPP CM supervised nodes.



S.No	Metrics Name	Description
12	numberOfSynchronizedNodes::cm-router-policy	Number of synchronized CPP nodes.
13	numberOfSuccessfulSubscriptions::er6000-router-policy	Number of successful CM subscriptions.
14	numberOfSupervisedNodes::er6000-router-policy	Number of CM supervised nodes.
15	numberOfSynchronizedNodes::er6000-router-policy	Number of synchronized nodes.

Table 11 DpMediation Metrics

S.No	Metrics Name	Description
1	numberOfActiveCellsCount::domain-proxy-sas-handler-code	Number of active cells managed by domain proxy.
2	numberOfMaintainedGrantsCount::domain-proxy-sas-handler-code	Number of authorized grants maintained by domain proxy.
3	numberOfFailedCbsdRegistrationsIncremental::domain-proxy-sas-handler-code_trendsUp	Number of failed CBSD registrations.
4	numberOfFailedConnectionAttemptsWithSasIncremental::domain-proxy-sas-handler-code_trendsUp	Number of failed http/tls connections counter of SAS.
5	numberOfRelinquishedGrantsIncremental::domain-proxy-sas-handler-code_trendsUp	Number of grants relinquished by domain proxy.
6	numberOfRevokedGrantsIncremental::domain-proxy-sas-handler-code_trendsUp	Number of grants revoked. That is, terminated, expired.



S.No	Metrics Name	Description
7	numberOfSuspendedGrantsIncremental::domain-proxy-sas-handler-code_trendsUp	Number of grants suspended by a SAS.
8	numberOfTerminatedGrantsIncremental::domain-proxy-sas-handler-code_trendsUp	Number of grants terminated by a SAS.
9	numberOfInactiveCellsCount::domain-proxy-sas-handler-code	Number of inactive cells managed by domain proxy.
10	numberOfRegisteredCbsdsCount::domain-proxy-sas-handler-code	Number of registered CBSDs.
11	numberOfValidGrantsCount::domain-proxy-sas-handler-code	Number of valid grants.
12	maxHbResponseTimePerMinute	Maximum time per minute taken to receive heartbeat responses from SAS.
13	minTxExpiryTimePerMinute	Minimum TxExpiryTime per minute given by SAS.
14	numberOfActiveCellsCount::netconf-session-releaser-handler	netconf-session-releaser-handler Number of active cells being managed by domain proxy.
15	numberOfMaintainedGrantsCount::netconf-session-releaser-handler	Number of authorized grants being maintained by domain proxy.
16	numberOfFailedCbsdRegistrationsIncremental::netconf-session-releaser-handler_trendsUp	Number of failed CBSD registrations.
17	numberOfFailedConnectionAttemptsWithSasIncremental::netconf-session-releaser-handler_trendsUp	Number of failed http/tls connections counter for SAS.



S.No	Metrics Name	Description
18	numberOfRelinquishedGrantsIncremental::netconf-session-releaser-handler_trendsUp	Number of grants relinquished by domain proxy.
19	numberOfRevokedGrantsIncremental::netconf-session-releaser-handler_trendsUp	Number of grants revoked. That is terminated, expired.
20	numberOfSuspendedGrantsIncremental::netconf-session-releaser-handler_trendsUp	Number of grants suspended by a SAS.
21	numberOfTerminatedGrantsIncremental::netconf-session-releaser-handler_trendsUp	Number of grants terminated by a SAS.
22	numberOfInactiveCellsCount::netconf-session-releaser-handler	Number of inactive cells managed by domain proxy.
23	numberOfRegisteredCbsdsCount::netconf-session-releaser-handler	Number of registered CBSDs.
24	numberOfValidGrantsCount::netconf-session-releaser-handler	Number of valid grants.
25	numberOfActiveCellsCount	Number of active cells managed by domain proxy.
26	numberOfMaintainedGrantsCount	Number of authorized grants maintained by domain proxy.
27	deregistrationRequestsCount	Number of deregistration requests to be sent to SAS.
28	deregistrationResponsesCount	Number of deregistration responses received from SAS.
29	EUtranFrequenciesDeletedCount	Number of EUtran cell frequencies deleted.



S.No	Metrics Name	Description
30	EUtranFrequencyRelationsDeletedCount	Number of EUtran cell frequency Relations deleted.
31	numberOfFailedCbsdRegistrationsIncremental	Number of failed CBSD registrations.
32	numberOfFailedConnectionAttemptsWithSasIncremental	Number of failed http/tls connections counter for SAS.
33	grantRequestsCount	Number of grant requests to be sent to SAS.
34	grantResponsesCount	Number of grant responses received from SAS.
35	numberOfRelinquishedGrantsIncremental	Number of grants relinquished by domain proxy.
36	numberOfRevokedGrantsIncremental	Number of grants revoked. That is terminated, expired or auto de-registered from SAS.
37	numberOfSuspendedGrantsIncremental	Number of grants suspended by a SAS.
38	numberOfTerminatedGrantsIncremental	Number of grants terminated by a SAS.
39	heartbeatRequestsCount	Number of heartbeat requests to be sent to SAS.
40	heartbeatResponsesCount	Number of heartbeat responses received from SAS.
41	numberOfInactiveCellsCount	Number of inactive cells managed by domain proxy.
42	numberOfRegisteredCbsdsCount	Number of registered CBSDs.
43	requestsPostedToSASCount	Number of requests posted to SAS.



S.No	Metrics Name	Description
44	spectrumInquiryRequestsCount	Number of spectrum inquiry requests to be sent to SAS.
45	spectrumInquiryResponsesCount	Number of spectrum inquiry responses received from SAS.
46	frequenciesChangedCount	Number of times change frequency performed via DPS.
47	setCbrsTxExpiryTimeCount	Number of times set CBRS transmission expiry time performed via DPS.
48	numberOfValidGrantsCount	Number of valid grants.
49	setCbrsTxExpiryTimeTimeRunningTotal	Set CBRS transmit expiry time on cell total time.
50	postRequestToSASTime	Time taken to send request and get a response from SAS.
51	getMOFromDPSTime	Time to get MO from DPS.
52	numberOfFailedAttemptsWithSas	Total number of failed attempts in contacting SAS.
53	totalNumberOfHbResponsesFromSAS	Total number of heartbeat responses received from SAS.
54	totalNumberOfHbToSAS	Total number of heartbeats to SAS.
55	totalNumberOfTransmitExpiryTimeSetOnNode	Total number of TransmitExpiry time set on the node.
56	totalHbResponseTimeFromSas	Total time taken to receive heartbeat responses from SAS.
57	totalTransmitExpiryTimePerHbResponseFromSas	Total TransmitExpiry time per heartbeat



S.No	Metrics Name	Description
		response received from SAS.
58	totalTransmitExpiryTimeSetOnNode	Total TransmitExpiry time set on the node.

Table 12 Nbalarmirp

S.No	Metrics Name	Description
1	alarmsSentToNotificationService	Number of alarms sent to NMS.

Table 13 SSO

S.No	Metrics Name	Description
1	activeSession	Number of active sessions in the system.
2	maxAllowedSessions	Max threshold of allowed active sessions in the system.

8.3 Access ESM Common Metrics

This section describes the Common Metrics that are collected by ESM. ESM collects Common Metrics for the Virtual Machines (VMs) where JBoss is running. These metrics are collected per minute basis. The Common Metrics are visible to all the users of ESM and no specific permissions are required to view them.

Prerequisites

The user is logged on to ESM.

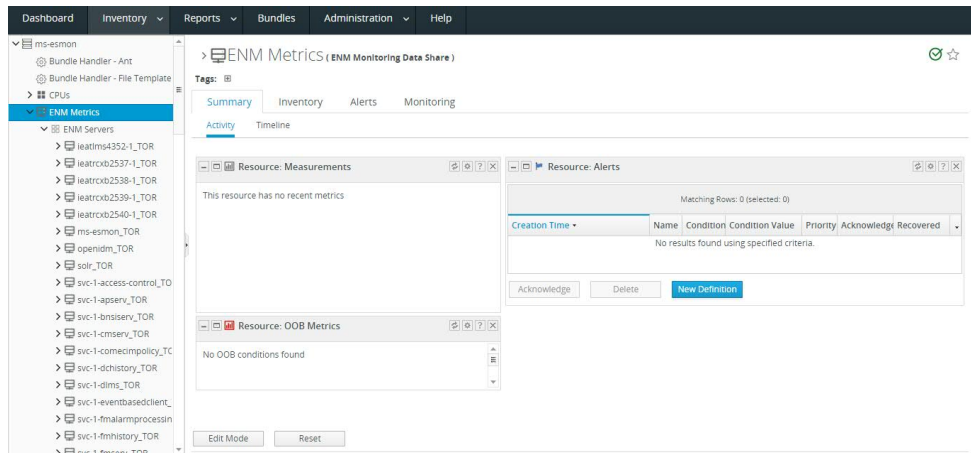
Steps

1. Click **Inventory**.

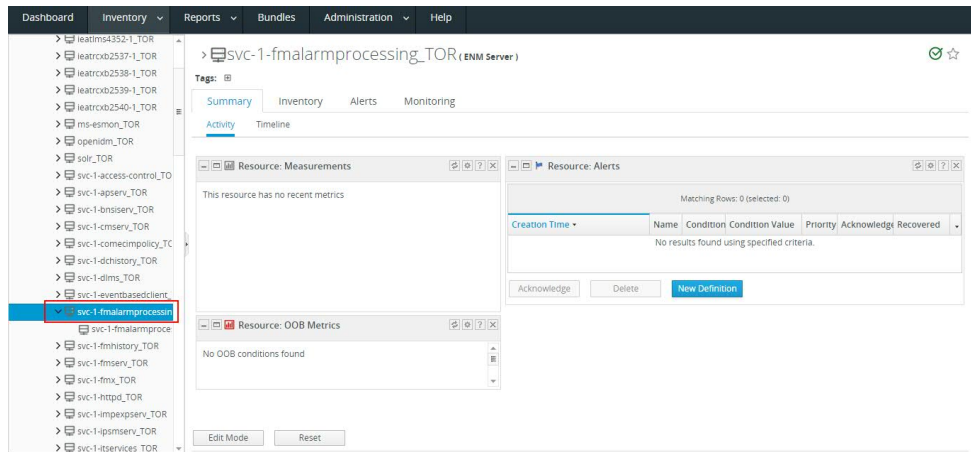


2. Click **Platforms**.
3. Select esmon platform.
4. Click **ENM Metrics**.

5. Click **ENM Servers**.

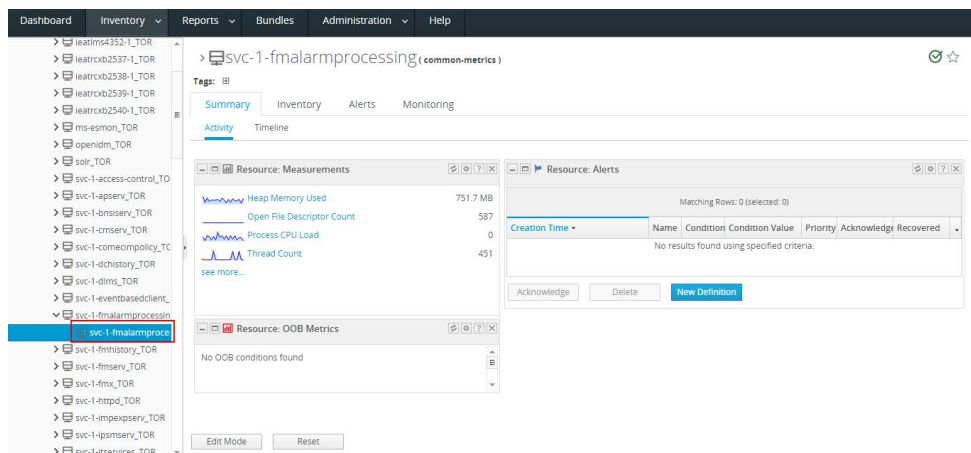


6. Click any VM.

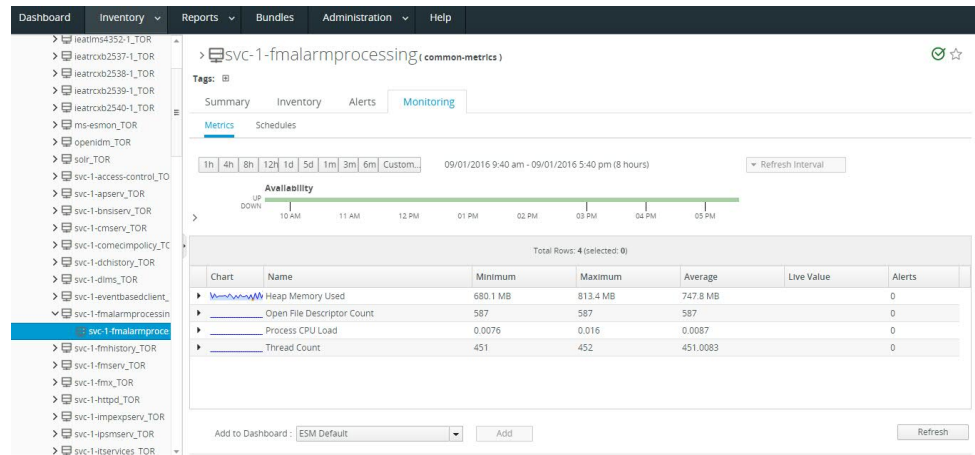


7. Click the immediate child resource of the VM.

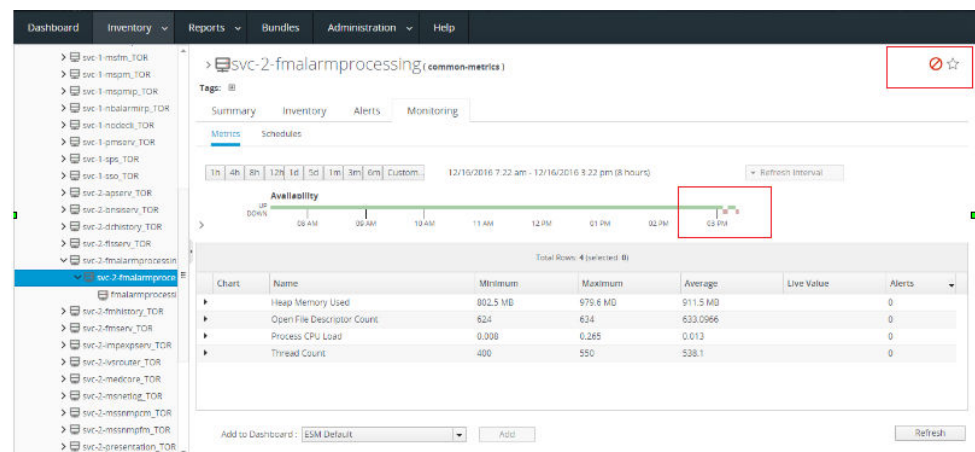
This displays the name of the VM.



8. Click **Monitoring** > **Metrics** to view all the metrics that are collected.



- Unavailability of instrumentation data for more than five minutes of a particular application is shown in red.



Results

The user is able to access Common Metrics that are collected by ESM.

8.3.1 ESM Common Metrics

The following table contains the list of Common Metrics that are collected by ESM.

Table 14 Common Metrics

S.No	Metric Name	Description
1	Heap Memory Used	The amount of used memory that is used by Java virtual machine
2	Open File Descriptor Count	The count of Open File Descriptors. A file descriptor is an



S.No	Metric Name	Description
		abstract indicator used to access a file or other input/output resource, such as a pipe or network connection.
3	Process CPU Load	The percentage CPU usage for the Java Virtual Machine process.
4	Thread Count	Number of threads of execution

8.4 Access VM Availability Metrics

ESM collects metrics for VM availability. It displays the availability of a particular VM in the form of 1's and 0's. 1 indicates VM is available, 0 indicates VM is unavailable.

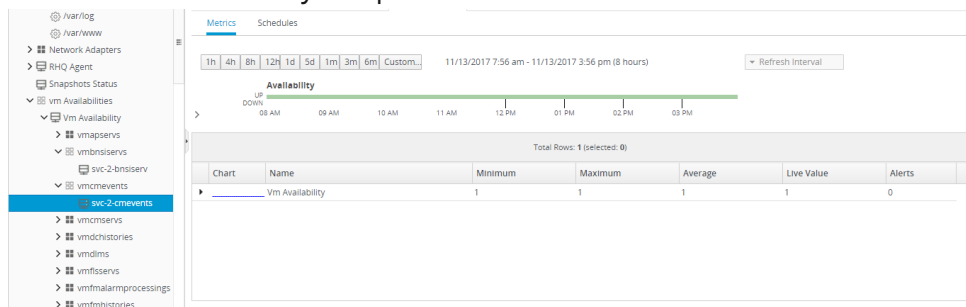
These metrics are visible to all the users of ESM, and no specific permissions are required to view them.

Prerequisites

The user is logged on to ESM.

Steps

1. Click **Inventory**.
2. Click **Platforms**.
3. Select **ms platform**
4. Click **vm Availabilities > Vm Availability**.
5. Click any VM.
6. Click **Monitoring > Metrics** to view all the metrics that are collected, which indicates the availability of a particular VM.



8.5 Access VM Group Availability Metrics

ESM collects metrics for VM Group availability. It displays the availability percentage of a similar type of VM's running on different blades. The percentage



is computed based on the number of active instances of a VM out of total deployed instances.

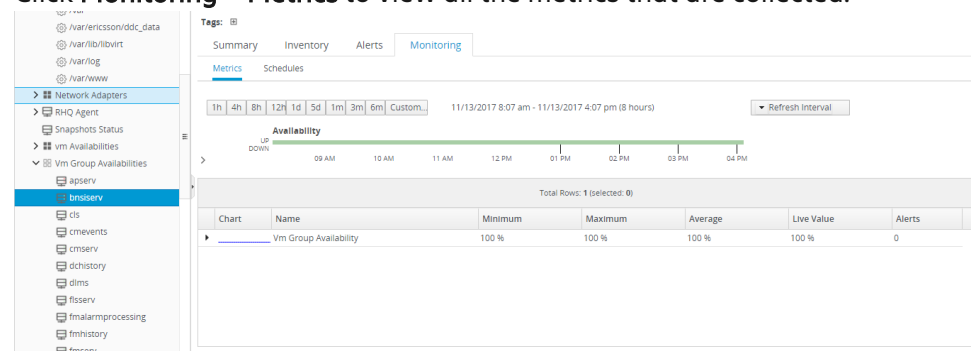
These metrics are visible to all the users of ESM and no specific permissions are required to view them.

Prerequisites

The user is logged on to ESM.

Steps

1. Click **Inventory**.
2. Click **Platforms**.
3. Select **ms** platform.
4. Click **vm Group Availabilities**.
5. Click any VM.
6. Click **Monitoring > Metrics** to view all the metrics that are collected.





9 View Resource Metrics

ESM users can view the metrics for a specified resource.

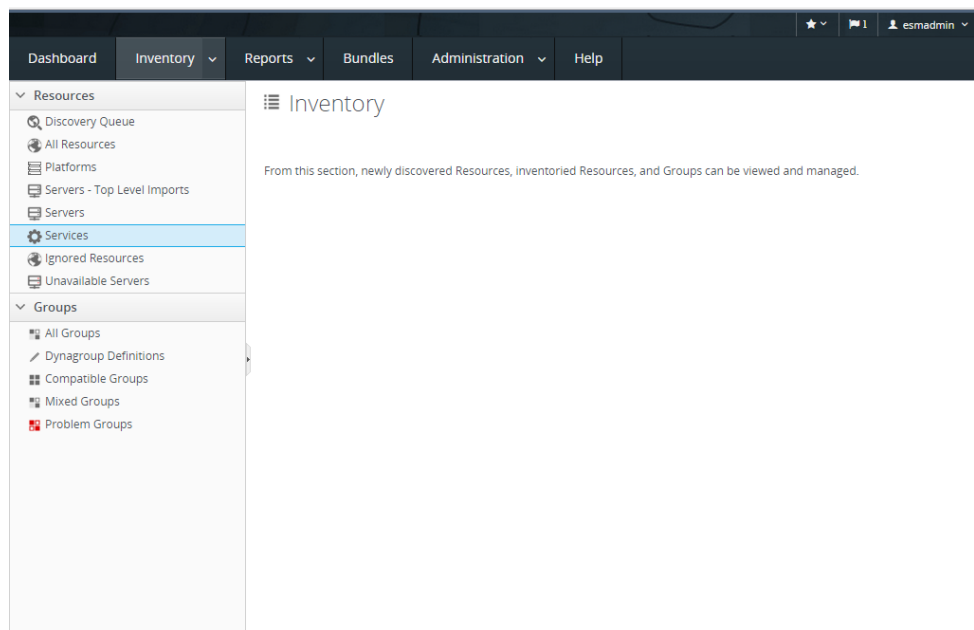
Viewing metrics for a specified resource is available for the three default ESM Users. They are collected on a per-minute basis.

Prerequisites

The user is logged on to ESM.

Steps

1. Log on to ESM.
2. Click **Inventory**.



3. Click **Platforms**.
4. Select any platform from the list.



The screenshot shows the 'Platforms' section of the ESM GUI. A table lists several platforms, with 'cloud-svc-1' selected. A tooltip for 'cloud-svc-1' displays the following information:

Name	Ancestry	Description	Type	Version	Availability
cloud-svc-1		Linux Operating System	Linux	Linux 2.6.32-504.54.1.e	✓

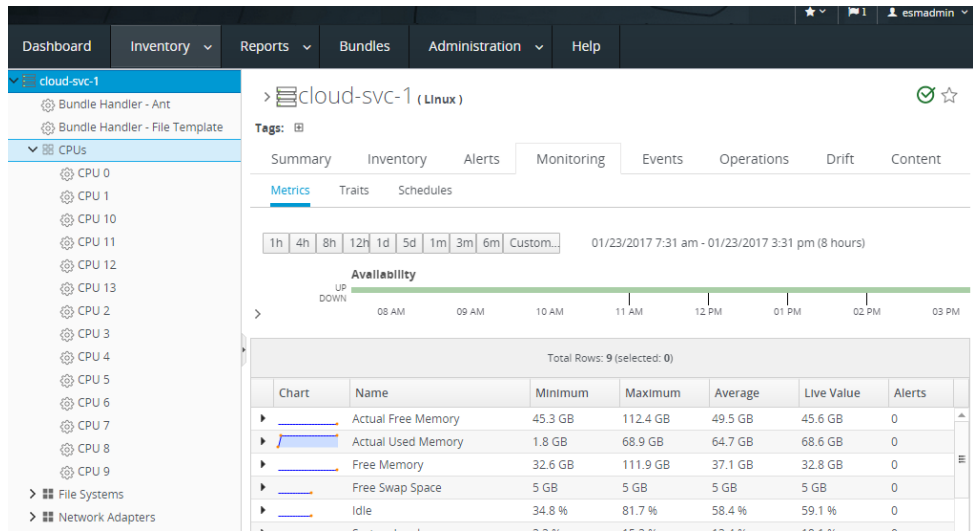
5. Click **Monitoring > Metrics** to view all metrics collected for this platform.

The screenshot shows the 'Metrics' page for the 'cloud-svc-1' platform. The 'Monitoring' tab is active, displaying a chart for 'Availability' and a table of metrics. The 'Availability' chart shows the platform is 'UP' from 08 AM to 03 PM. The 'Metrics' table is as follows:

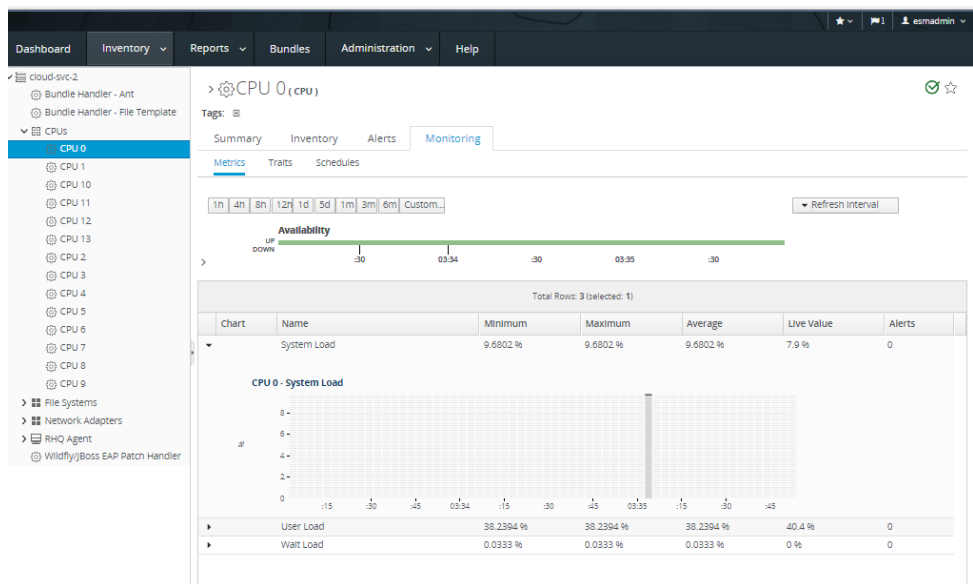
Chart	Name	Minimum	Maximum	Average	Live Value	Alerts
▶	Actual Free Memory	45.3 GB	112.4 GB	49.5 GB	45.6 GB	0
▶	Actual Used Memory	1.8 GB	68.9 GB	64.7 GB	68.6 GB	0
▶	Free Memory	32.6 GB	111.9 GB	37.1 GB	32.8 GB	0
▶	Free Swap Space	5 GB	5 GB	5 GB	5 GB	0
▶	Idle	34.8 %	81.7 %	58.4 %	59.1 %	0
▶	System Load	3.3 %	15.3 %	13.4 %	18.1 %	0

Note: CPU Metrics in ESM GUI and server do not match as the CPU metrics continuously change.

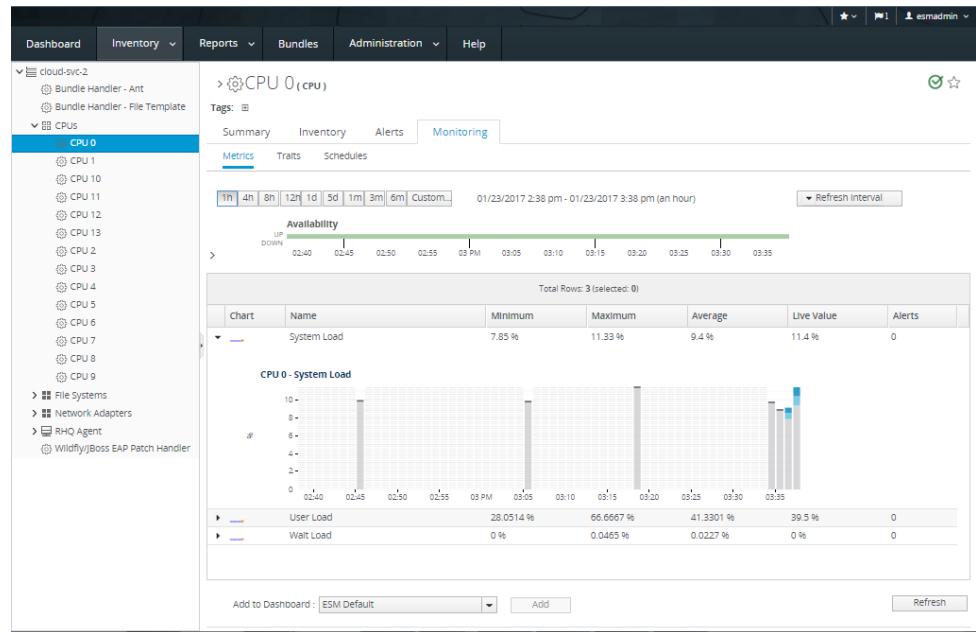
6. Select a child resource from the list on the left to view information specific to that resource.



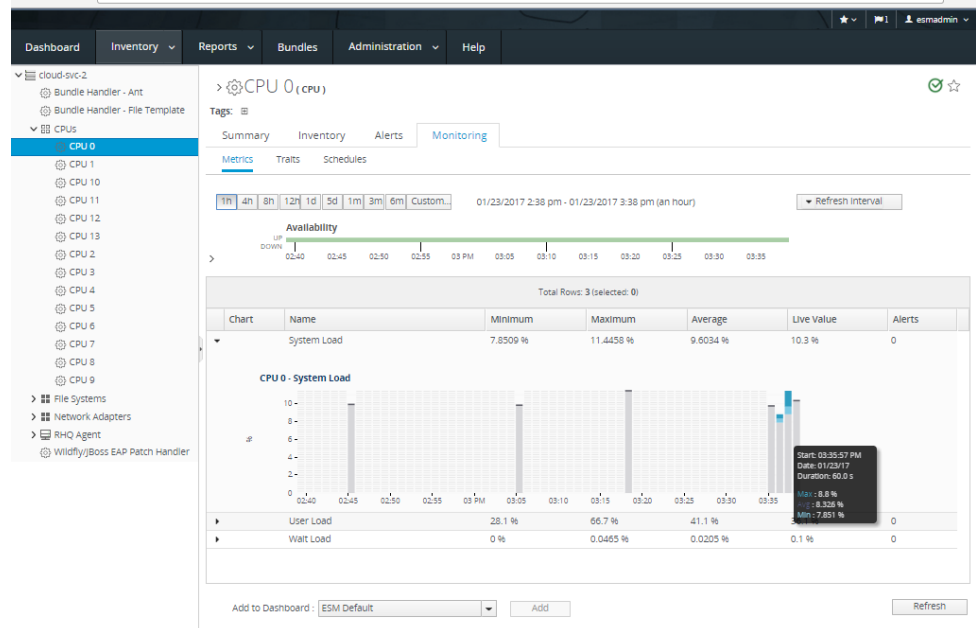
- 7. Click the black arrow next to each metric to display a graph of metric readings over time.



- 8. Use the 1 h, 4 h, 8 h, 12 h buttons to choose the appropriate time range. The following graph shows the same metric as the one above, but using a different time range (1d - last day).



9. Hover on the bar to view the graph and the values it represents.





10 Enabling and Disabling Metrics of a Specific Resource

Metrics can be enabled and disabled for a specific resource.

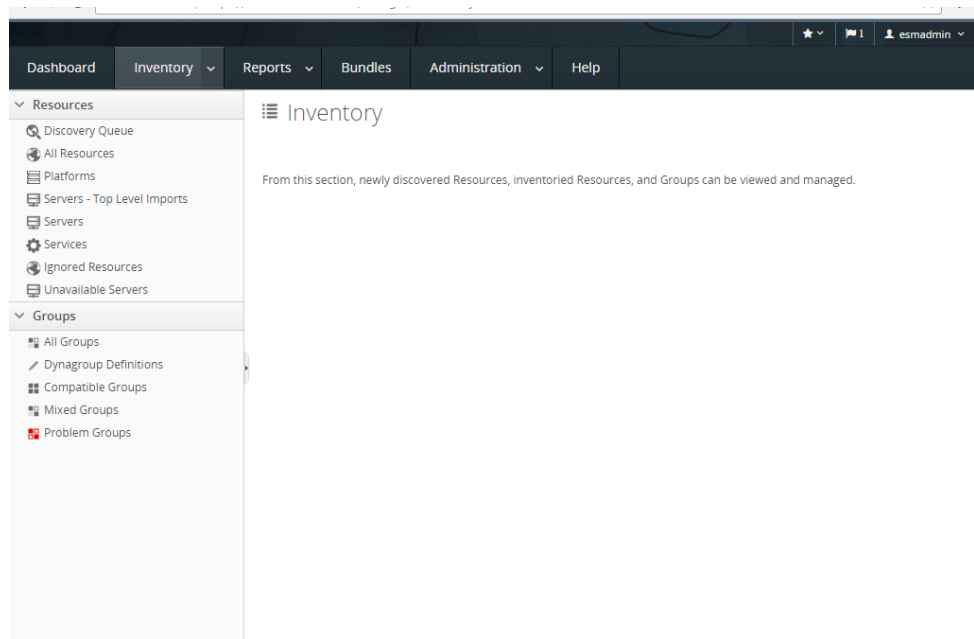
The enable operation is performed when the user wants to collect a specific metric for a resource. The disable operation is performed when the metrics for a particular resource are no longer required.

Prerequisites

The user is logged on to ESM. Enabling/disabling of metrics can be done by an administrator.

Steps

1. Log on to ESM
2. Click **Inventory**.
3. Select the resource type in the **Resources** menu on the left and browse/search for the required resource.



4. Click the **Monitoring** tab on the resource entry.



5. Click **Schedules**.
6. Select the metrics to enable or disable.

The screenshot shows the 'Monitoring' tab for resource 'cloud-ms-1' (Linux). The 'Schedules' sub-tab is active, displaying a table of metrics. The table has columns for Metric, Description, Type, Enabled?, and Collection Interval. Below the table, there is a 'Collection Interval' dropdown set to 'minutes' and a 'Set' button. At the bottom, there are 'Enable', 'Disable', and 'Refresh' buttons.

Metric	Description	Type	Enabled?	Collection Interval
Actual Free Memory	The actual total free system memory (includes unallocated memory as well as available buffer and cache memory)	measureme	<input checked="" type="checkbox"/>	10 minutes
Actual Used Memory	The actual total used system memory (includes buffer and cache memory)	measureme	<input checked="" type="checkbox"/>	10 minutes
Architecture	Hardware architecture of the platform	trait	<input checked="" type="checkbox"/>	24 hours
Distribution Name	name of the Linux distribution	trait	<input checked="" type="checkbox"/>	24 hours
Distribution Version	version of the Linux distribution	trait	<input checked="" type="checkbox"/>	24 hours
Free Memory	The total free system memory (does not include buffer or cache memory)	measureme	<input checked="" type="checkbox"/>	10 minutes
Free Swap Space	The total free system swap	measureme	<input checked="" type="checkbox"/>	20 minutes
Hostname	Name that this platform is known as	trait	<input checked="" type="checkbox"/>	24 hours
Idle	Idle percentage of all CPUs	measureme	<input checked="" type="checkbox"/>	20 minutes

Results

Metrics for a specific resource are disabled or enabled.



11 ENM System Monitor Alerts

ESM can collect, analyze, and alert on the data that it collects. Alert definitions can be created on every resource and metric combination in the system; for example, it is possible to create an alert on CPU 1 of svc-1 for the System Load metric.

The application recognizes two main types of alarms: alerts that are internal to ESM and FM alarms that appears in ENM Fault Management system. Internal alerts are visible to all users of ESM but are not shown in any other part of ENM. ESM is capable of forwarding its alerts to ENM Fault Management as Alarms. Alerts that are forwarded appear both in ESM and in FM.

An Alert Definition is made up of a number of characteristics.

General Properties

The following general properties are associated with the alert:

- Name: human-readable name.
- Description: textual description.
- Priority: severity level.
- Enabled: whether the alert is currently enabled.

Conditions

A set of conditions that cause the system to raise this alert.

- Fire alert when: whether the alert should fire when ALL of the listed conditions are satisfied or if ANY one is satisfied.

Notifications

A list of notifications that the system sends out in addition to displaying the alert on the ESM dashboard.

Recovery

Not supported in ESM.

Dampening

Not supported in ESM.



Table 15 Conditions Types

S.No	Condition Type	Description
1	Availability Change	Monitor the availability of a resource and alert when it enters a specific state, for example "goes down".
2	Availability Duration	Monitor the availability of a resource over a specified duration.
3	Measurement Absolute Value Threshold	Alert when the value of a metric is below, at, or above a specific value.
4	Measurement Baseline Threshold	Alert when the value of a metric is below, at, or above a specific baseline expressed as a percentage.
5	Measurement Value Change	Alert when the value of a metric changes.
6	Measurement Value Range	Alert when the value of a metric falls within the specified range.
7	Trait Value Change	Alert when a trait of a resource changes to the specified value.

Table 16 Notifications Senders

S.No	Condition Type	Description
1	FM Alert	Raise an alarm in ENM Fault Management.
2	FM Clear Alert	Clear a previously raised alarm in ENM Fault Management.

Table 17 Alert Severity Mapping ESM GUI and FM Alarm Monitor

S.No	ESM GUI	FM Alarm Monitor
1	Low	Minor
2	Medium	Major
3	High	Critical

— RELATED INFORMATION —

[11.1 View Alert Information on page 46](#)

[11.2 Create FM Alert Notifications on page 48](#)

[11.3 Create Internal Alerts on page 58](#)

[11.4 Update an Existing Alert on page 62](#)

[11.5 Delete Alert Definition Template of a Given Resource on page 63](#)



11.1 View Alert Information

Alerts are raised when a metric meets the threshold value specified in the conditions of alert definition.

All users can view this alert information.

Prerequisites

- The user is logged on to ESM.
- An alert has been raised by the system.

Expected Result

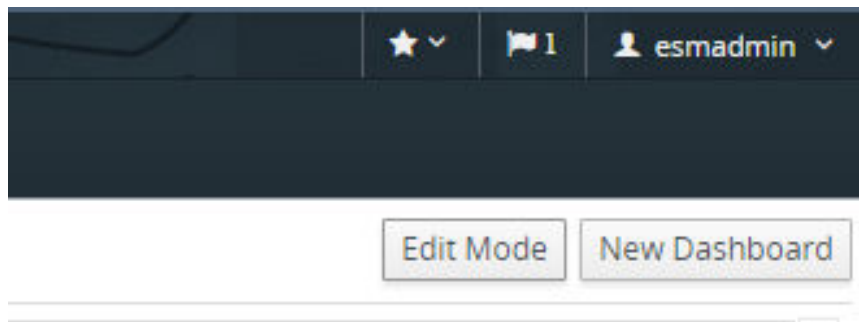
You can view information related to alerts and the affected resources.

Steps

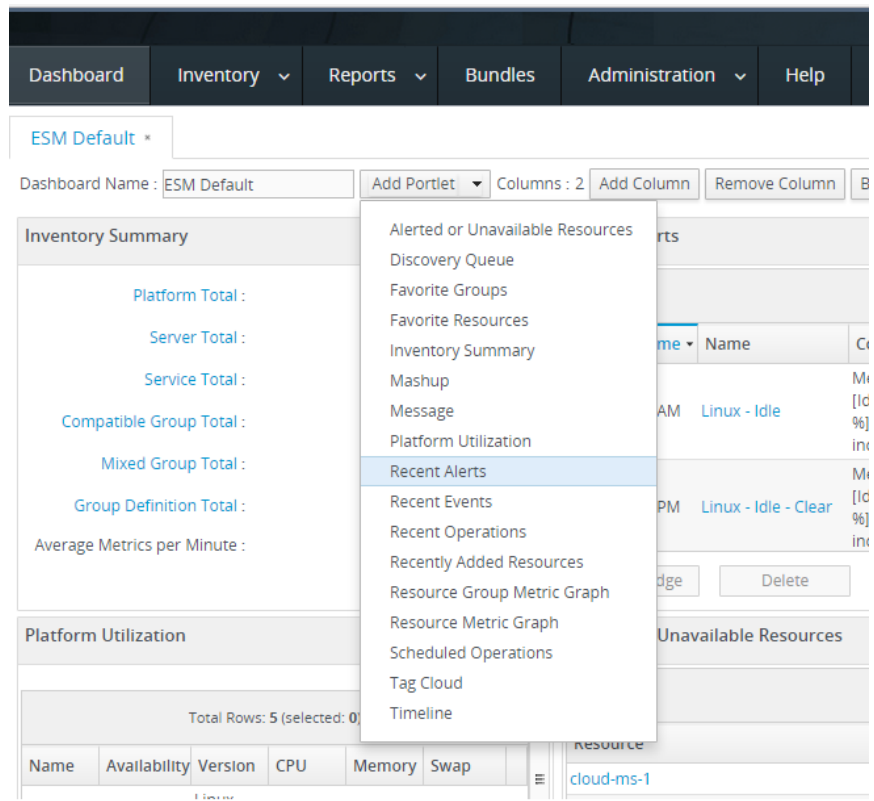
1. Log on to ESM
2. Click **Dashboard**.
3. Locate the **Recent Alerts** view.

Creation Time	Name	Condition Text	Condition Value	Priority	Acknowledge	Recovered	Resource
3/3/16 3:02 PM	sample alert	Metric Value Threshold [Free Space > 0.0 kB]	12.5 GB	High		/	
3/3/16 3:02 PM	sample alert	Metric Value Threshold [Free Space > 0.0 kB]	12.5 GB	High		/	
		Metric Value Threshold [Free					

4. To enable **Recent Alerts**, if the view is not displayed:
 - a. Click **Edit Mode** located on the top-right corner of the screen.

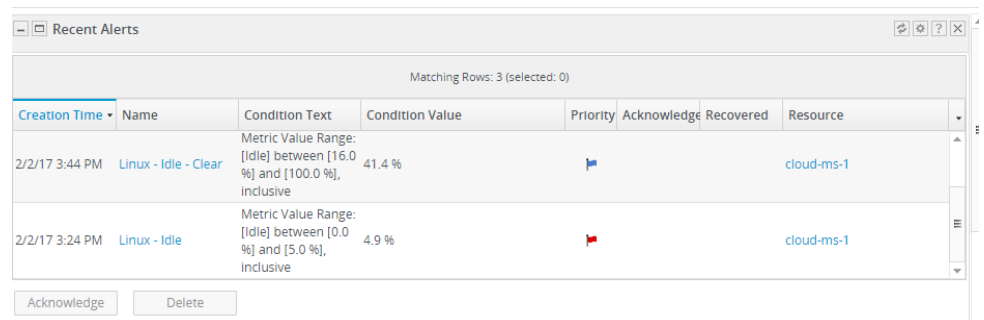


- b. Select **Add Portlet > Recent Alerts**.



c. Click **View Mode** located on the top-right corner of the screen.

5. Double-click on any alert listed on the **Recent Alerts** portlet to view its details.



6. The details shown include general properties, thresholds, and recorded values, and notifications that are triggered as a result.



11.2 Create FM Alert Notifications

The user can see the raised FM Alert on Alarm Monitor page by creating ESM alerts that are forwarded to ENM FM Alarm Monitor.

Prerequisites

User is either an esmadmin or esmalertadmin. Only esmalertadmin and esmadmin users are allowed to perform this task.

To monitor a resource with FM Alarm escalation and de-escalation, multiple alerts (including a clear alert) with different priorities have to be set up in ESM.

Each time an alert is raised, that particular alert is disabled and all other alerts on that resource metric are enabled. This is done to avoid raising multiple alerts on a single, continued threshold breach.

There is only one alarm created at the FM side on a particular metric on a particular resource, whereas there is one alert raised at the ESM side for each priority of that metric. The same alarm at FM is escalated, de-escalated, or cleared based on the condition met.

Every FM Alarm raised from ESM can be found in the ESM Alert History tab on the Alerts page.

To forward an ESM alert to FM as an alarm, the user must set its General Properties, Conditions, and Notification details.

Example

- This example goes through the process of creating an FM Alarm on a file system resource `/dev/shm` (on its Used Percentage metric).
- Four alert types are covered: Low, Medium, and High priority alerts as well as a Clear alert.
- The following thresholds are used:
 - Low: 50% to 70%
 - Medium: 70% to 90%
 - High: 90% to 100%
 - Clear: 0% to 50%

When the Used Percentage is within the given threshold, a corresponding alert is raised.



Steps

1. Log on to ESM as esmadmin or esmalertadmin user.
2. Click **Inventory**.
3. Click **Platforms**.
4. Select **esmon**.
5. Select **esmon > File Systems > /dev/shm** on the sidebar.
6. Click **Alerts**.

The screenshot shows the ENM System Monitor Alerts interface. The top navigation bar includes Dashboard, Inventory, Reports, Bundles, Administration, and Help. The left sidebar shows the esmon platform selected, with File Systems > /dev/shm highlighted. The main content area displays the Alerts tab for /dev/shm (File System). The Alerts tab is active, showing a table of alerts. The table has columns for Name, Description, Creation Time, Modified Time, Enabled, Priority, Parent, and Protected. There are 6 rows of alerts, all created on Jan 21, 2017 at 3:40:55 AM. The alerts include File System - Used Percentage exceeded, File System - Options Changed, and File System - Used Percentage - Clear. The table also shows a 'Total Rows: 6 (selected: 0)' and buttons for New, Enable, Disable, Delete, and Refresh.

Name	Description	Creation Time	Modified Time	Enabled	Priority	Parent	Protected
File System - Used Percentage	File System Threshold exceeded	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✓	High	View Template	No
File System - Used Percentage	File System Threshold exceeded	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✓	High	View Template	No
File System - Options	File System Mode Changed	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✓	High	View Template	No
File System - Options - Clear	File System Mode Changed	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✗	High	View Template	No
File System - Used Percentage - Clear	File System Threshold exceeded	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✗	High	View Template	No
File System - Used Percentage	File System Threshold exceeded	Jan 21, 2017 3:40:55 AM	Jan 21, 2017 3:40:55 AM	✓	High	View Template	No

7. Click **New** to create a new alert.
8. Enter the required name of the Alert in the **Name** field and fill in the description.
For example, see the [Create Alert for Disk Space](#) on page 50.
9. Select the required priority level from the drop-down list.
10. Create a **Clear** alert by using the clear tag, prefixed by Name (MetricName - Clear).
For an example, see [Create Clear Alert](#) on page 54.
11. ESM enables users to Acknowledge and Delete the alerts in the ESM GUI.

Acknowledging and Deleting the alerts in ESM GUI does not modify alarms state in FM alarm monitoring GUI.



Note: OPIs are not available for User Created Alerts.

Results

The alerts are displayed on the ESM Dashboard and ENM FM Alarm Monitor page if the thresholds are breached.

11.2.1 Create Alert for Disk Space

The following example shows how to create an alert for a disk space scenario.

1. Enter **Low on free space** in the **Name** field, **/dev/shm is low on free space** in the **Description** field, and select **Low** from the **Priority** drop-down list.

> /dev/shm (File System)

Tags:

Summary Inventory Alerts Monitoring

Definitions History

« Back to List

General Properties Conditions Notifications Recovery Dampening

Name :

Description :

Priority :

Enabled : Yes No

Note: It is mandatory to fill the **Description** field as it represents the Specific Problem in FM Alarm.

2. Click the **Conditions** tab.
3. Click **Add**.



4. Select **Measurement Value Range** in the **Condition Type** field, **Used Percentage** from the **Metric** drop-down list, and **Inside, Exclusive** from the **Comparator** drop-down list. Enter **50** to the **Low Value** field and **70** to the **High Value** field.

Add Condition

Condition Type : Measurement Value Range

Compares a metric value to a given low-high value range.

Metric : Used Percentage

Comparator : Inside, exclusive

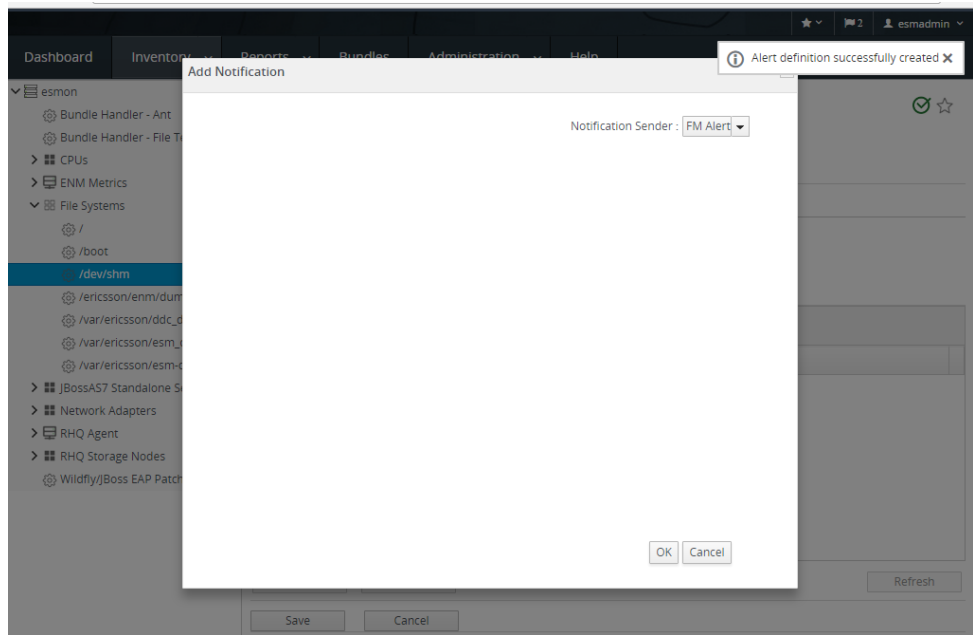
Low Value : 50

High Value : 70

Base Units : %

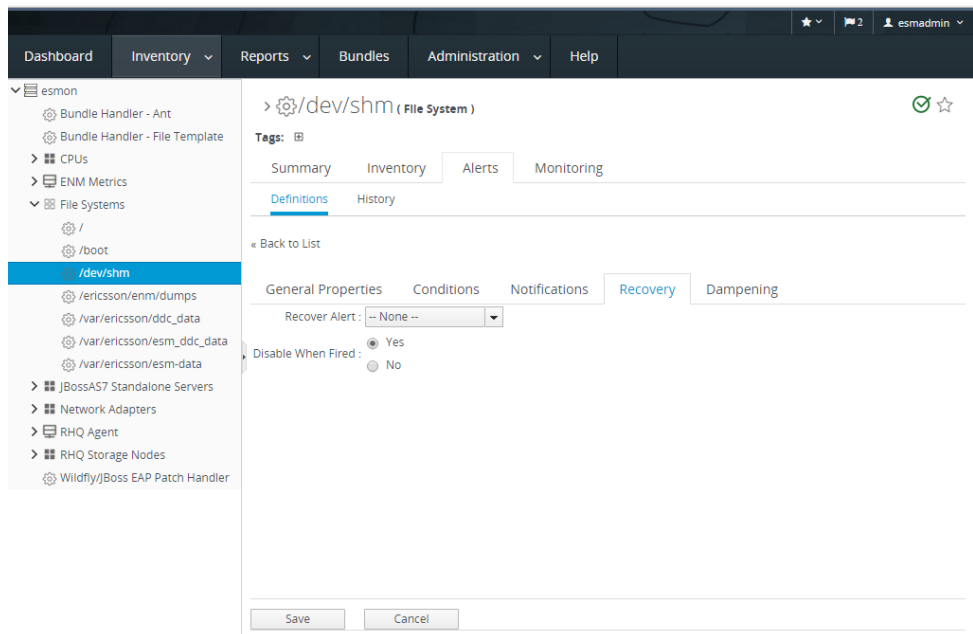
OK Cancel

5. Click **OK**.
6. Click **Notifications**.
7. Click **Add**.
8. Select **FM Alert** from the **Notification Sender** drop-down list and then click **OK**.



Note: Except for FM Alert and FM Clear Alert, the other options in drop down are not supported.

9. Click **Recovery**.
10. Select the **Yes** for **Disable When Fired**.



11. Click **Save** to store this alert.
12. Click **Back to List** to return to the list of alerts.



13. Follow the same procedure to create Medium and High priority alerts.
Only the Priority and Low/High values are changed.

Example 1 Medium Priority Alert

Add Condition [X]

Condition Type : Measurement Value Range ▼

Compares a metric value to a given low-high value range.

Metric : Used Percentage ▼

Comparator : Inside, exclusive ▼

Low Value : 70

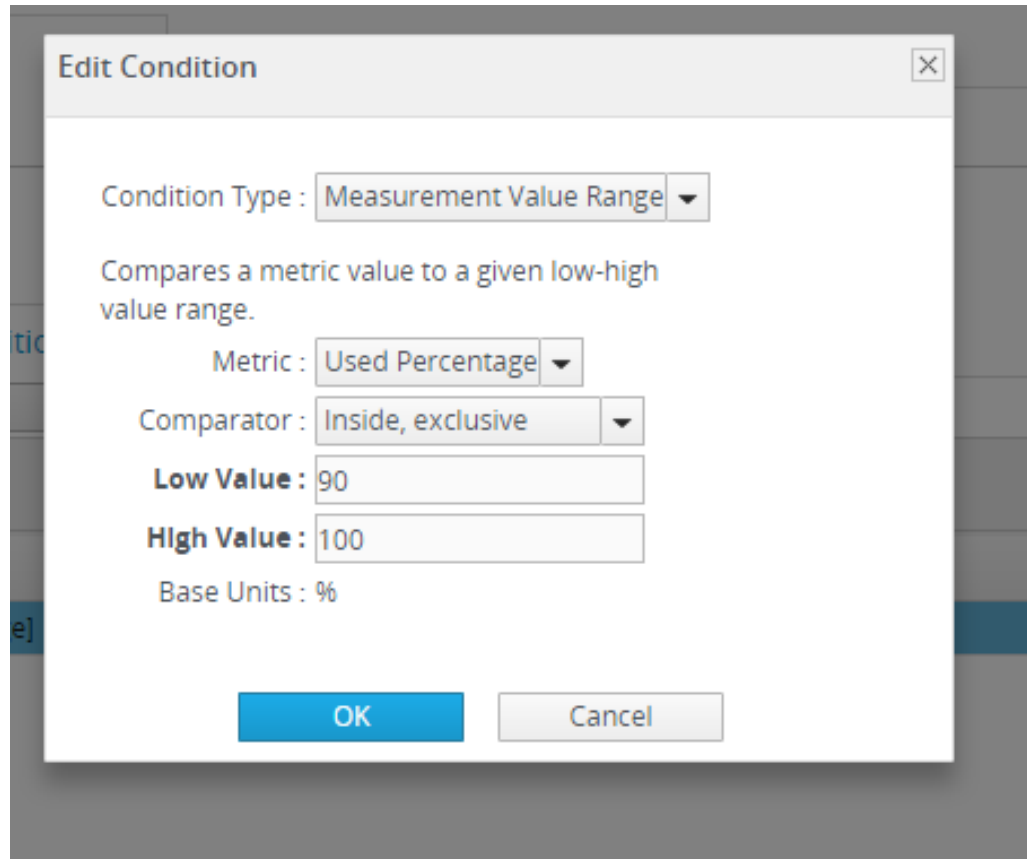
High Value : 90

Base Units : %

OK Cancel



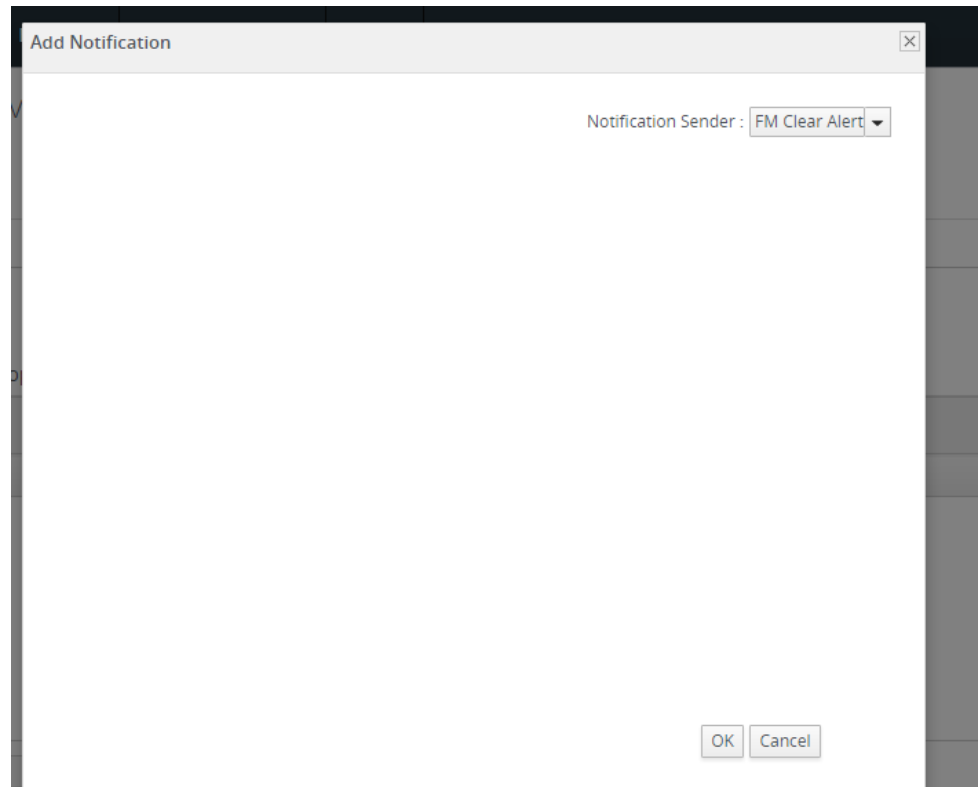
Example 2 High Priority Alert



11.2.2 Create Clear Alert

The following example shows how to create a Clear alert.

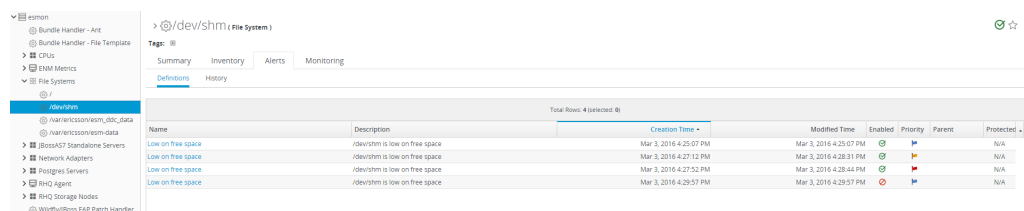
1. Set the **Priority** to **Low** and **Enabled** to **No** in the **General Properties** tab.
2. When adding a new condition, enter **0** to the **Low Value** field and **50** to the **High Value** field.
3. In the **Notification** tab, select **FM Clear Alert** from the **Notification Sender** drop-down list.



4. For each alert, select the **Yes** for **Disable When Fired** in the **Recovery** tab.

Results

With all the steps completed, the **Alerts > Definitions** tab for that resource is displayed as shown in the following image.



11.2.3 View Alarm on FM

To view the alarm on FM, do the following steps.

Prerequisites

The user is logged into the ENM launcher page as an administrator.



Steps

1. Open the Alarm Monitor from the ENM launcher page.
2. Open **Network Explorer > Search for managementsystem > Select ENM Object > Return Selected managed object.**
3. Click **Select on ENM** and then **Apply.**

Example

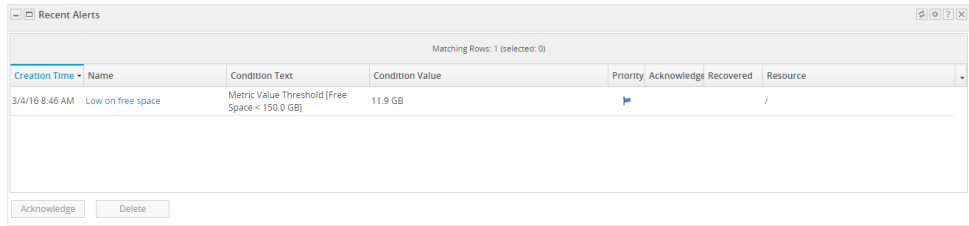


Figure 1 FM Alert Notification Displayed in ESM

Example

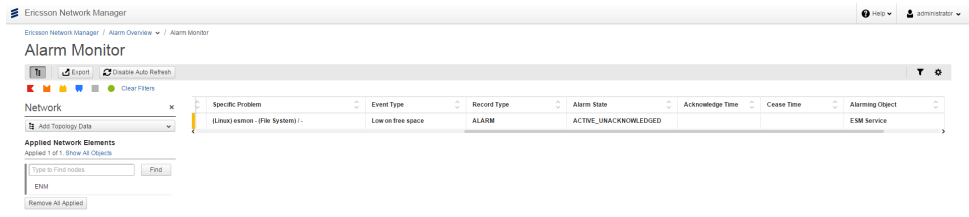
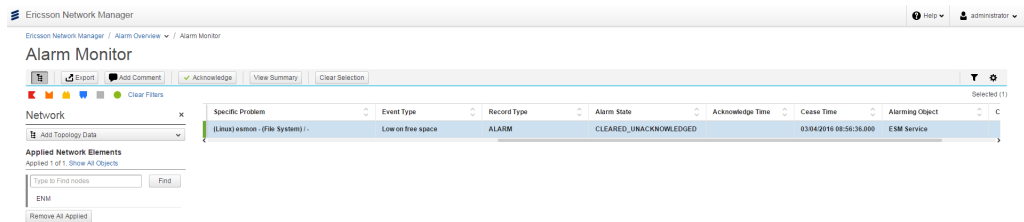


Figure 2 FM Alert Notification Displayed in ENM Alarm Monitor

Results

Once a Clear alarm is sent from ESM, its **Alarm State** in Alarm Monitor changes to **CLEARED** and user can remove it from the list by acknowledging it as shown in the following figure:





Example 3 Before Deletion

Matching Rows: 479 (selected: 1)

Creation Time	Name	Condition Text	Condition Value	Priority	Acknowledge	Recovered	Resource
8/5/16 12:51 PM	Sample Alert	Metric Value Range: [Used Percentage] between [0.0 %] and [70.0 %], exclusive	5.0 %				/ericsson/configuration_ma
8/5/16 12:51 PM	Sample Alert	Metric Value Range: [Used Percentage] between [0.0 %]	1.0 %				/var/ericsson

Acknowledge Delete

Figure 3 Alert ON ESM GUI

Alarm Monitor

Export Add Comment Acknowledge Clear Go To... View Summary Clear Selection

0 60 0 1 0 0

Network Add Topology Data

Applied Network Elements Applied 1 of 1. Show All Objects

Type to Find nodes Find ENM Remove All Applied

Specific Problem	Event Type	Record Type
(Linux) leatrcxb4371-1 - (File...	Sample Alert	ALARM
(Linux) leatrcxb4371-1 - (File...	Sample Alert	ALARM
(Linux) leatrcxb4371-1 - (File...	Sample Alert	ALARM
(Linux) leatrcxb4371-1 - (File...	Sample Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM
(Linux) leatrcxb4371-1 - (CP...	Test Alert	ALARM

Alarm Summary

Severity: MAJOR

Record type: ALARM

Previous Severity: UNDEFINED

Event Time: 08/05/2016 08:21:17

Event Type: Sample Alert

Specific Problem: (Linux) leatrcxb4371-1 - (File System) ericsson/configuration_management/Upgra deldependence -

Probable Cause:

Acknowledgement:

Acknowledge Time:

Cease Time:

Object Of Reference: ESM Service

Figure 4 Alarm ON FM GUI

Example 4 After Deletion
Alarm is not deleted from FM GUI.

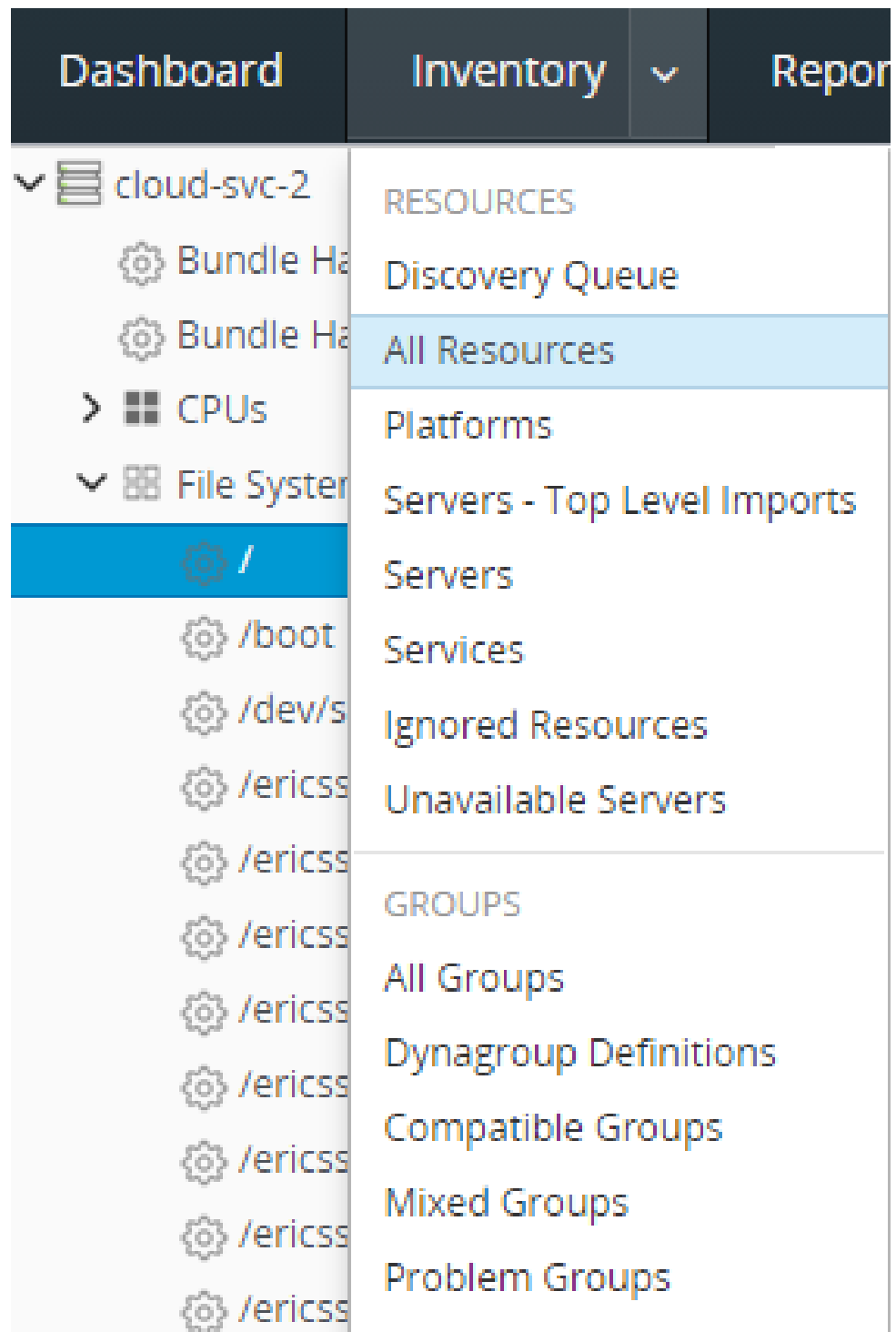
Recent Alerts

Matching Rows: 478 (selected: 0)

Creation Time	Name	Condition Text	Condition Value	Priority	Acknowledge	Recovered	Resource
8/5/16 12:51 PM	Sample Alert	Metric Value Range: [Used Percentage] between [0.0 %] and [70.0 %], exclusive	1.0 %				/var/ericsson
8/5/16 12:51 PM	Sample Alert	Metric Value Range: [Used Percentage] between [0.0 %]	3.0 %				/ericsson/enm/dumps

Acknowledge Delete

Figure 5 ESM GUI



3. Select a resource from the list.
4. Click **New**.
5. Enter **Name**, **Description**, and select **Priority** on the **General Properties** tab.



> / (File System)

Tags:

Summary Inventory **Alerts** Monitoring

Definitions History

« Back to List

General Properties Conditions Notifications

Name :

Description :

Priority :

Enabled : Yes No

6. Click **Conditions**.
7. Choose when to fire the alert: when all conditions are true, or if any one is true.

General Properties **Conditions** Notifications Recovery Dampening

Fire alert when :

ANY
ALL

Condition

Total Rows: 0 (selected: 0)

No items to show

8. Select **Add** to add a new condition.



- Select a condition type, if applicable select the metric and enter a threshold value.

Note: All the resources may not have the same list in **Condition Type** drop-down. They may vary from one resource to another based on the metrics that are collected for that particular resource.

For example, if the Metric collected for a resource is only Availability then the Condition type drop-down only contains Availability Duration and Availability Change.

Add Condition
✕

Condition Type :

Specify the threshold value that, when violated, triggers the condition. The value you specify is an absolute value with an optional units specifier.

Metric :

Comparator :

Metric Value :

Base Units : KB

Note: The Metric Value Range while defining an internal alert the default thresholds for CPU, Heap Memory, Total Memory are in Bytes instead of %.

- Click **OK** to add the condition, **Cancel** to discard it.
- Click **Save** to add the new Alert, **Cancel** to discard it.

Results

Note: There may be a delay in raising threshold alert. Click **monitoring tab** to raise an alert if there is delay.



11.4 Update an Existing Alert

This section describes how to edit (update or disable) an alert that is already created.

Only the administrator and Alert administrator can update an existing alert.

Prerequisites

- The user is logged on to ESM.
- An alert is already created.

Steps

1. Select a pre-existing alert.
2. Click on **Edit**.

> CPU 1 (CPU)

Tags: [x]

Summary Inventory Alerts Monitoring

Definitions History

« Back to List

General Properties Conditions Notifications Recovery Dampening

Fire alert when : ANY

Total Rows: 1 (selected: 0)

Condition

Metric Value Range: [System Load] between [90.0 %] and [95.0 %], exclusive

Add Delete Edit Condition

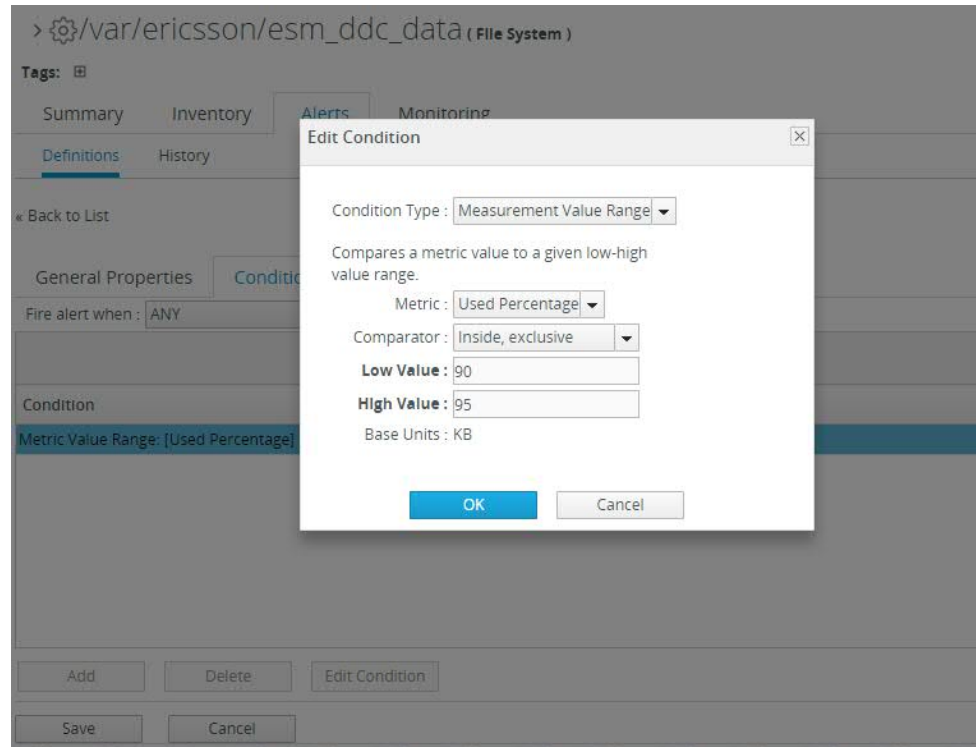
Edit

3. Enter the values which you wish to change under **General Properties** > **Conditions** > **Notification** > **Recovery** tabs.

Note: Changing the value of name, priority or description leads to inconsistent behavior. It is strongly recommended not to change these fields for default alert definitions.



4. Click **Save**.



Note: There is a limitation while editing the Condition of Alert. Editing Condition does not display the proper base unit.

During the creation of an alert if the base unit is defined as Percentage, it is displayed as KB when updating the alert.

Workaround: Click on the **Condition** Tab and enter the value enter the required value, click **Save**. The updated values is automatically saved as Percentage even if the base unit is displayed as KB.

5. To disable an existing alert:

- a. Click **Inventory > Platform > Select "Db Node" > File system > / ericsson/esm_ddc_data** .
- b. Click **Alerts Tab > Definitions**.
- c. Select all the alert definitions with the description File System Used Percentage and click **Disable**.

11.5 Delete Alert Definition Template of a Given Resource



Steps

1. Login to ESM GUI, and select **Administration**.
2. Under the **Configuration** tab, select **Server Plugins**.
3. Select the **Alert Plugin** configuration, then select **Disable**.
Note: Do not click on the hyperlink.
4. Select **Inventory > Platform**.
5. Select the required *<Platform>* *>* *<resource>* *>* select **Alerts**.
6. Select the required alert definition template, then click **Delete**.
Note: Do not click on the hyperlink.

11.5.1 Enable Alert Configuration Plugin

1. Log on to ESMON and backup the JAR file.

```
cp /opt/rhq/rhq-server/modules/org/rhq/server-startup/main/deployments/rhq.e →  
ar/rhq-serverplugins/alert-configurer-plugin-1.29.1.jar /tmp/
```

2. Log on to ESM GUI and navigate to **Administration > Server Plugins > Delete alert configuration plugin** and then wait for 10 to 15 minutes to get it flushed from server.
3. Run the following command in ESMON:

```
cp /tmp/alert-configurer-plugin-1.29.1.jar /opt/rhq/rhq-serve →  
r/plugins/
```

4. In ESM GUI, navigate to **Administration > Server Plugins**, select **Scan for Updates**, and check if the plugin jar is available.

Note: If any alert definition template in **Administration > Alert Definition Templates** is edited, the deleted alarm is re-generated.



12 View Default ESM Alert Thresholds

This section describes how to check the default thresholds for file system and Linux templates. The templates are visible to all the users of ESM and no specific permissions are required to view them.

By default, the conditional alerts. That is, **File System - Used Percentage**, **Linux - Idle**, and **File System - Options** are enabled and **Clear alert** is disabled. Once the conditional alert is triggered, then the **Clear alert** is enabled.

— RELATED INFORMATION —

[12.1 View File System Alert Thresholds on page 65](#)

[12.2 View Linux Alert Thresholds on page 68](#)

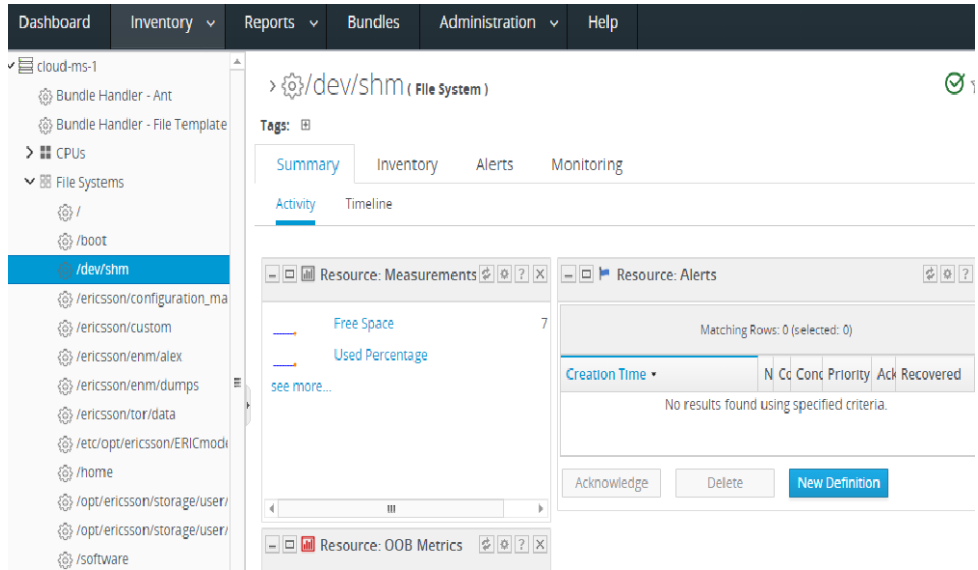
[12.3 View Snapshots Status Alert Thresholds on page 70](#)

[12.4 View VM Group Availability Alert Thresholds on page 72](#)

[12.5 Edit Conditions on page 74](#)

12.1 View File System Alert Thresholds

1. Click **Inventory**.
2. Click **Platforms**.
3. Select any Platform from the **Platforms** list.
4. Click the **File System** tab on the left side panel and select one of the available file systems.



Note: RHQ supports up to NFS V2.

5. Click **Alerts**.

File System Templates are found on all the File Systems.

File System Options - The alert is triggered when the permissions of any file system changes such as read or write.

File System Used Percentage - The alert is triggered when the Used Percentage crosses a certain threshold limit.

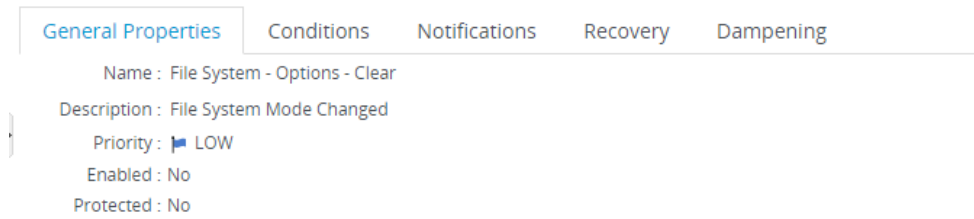
Summary Inventory **Alerts** Monitoring

Definitions History

Total Rows: 6 (selected: 0)							
Name	Description	Creation Time	Modified Time	Enabled	Priority	Parent	Protected
File System - Used Percentage - Clear	File System Threshold exceeded	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No
File System - Used Percentage	File System Threshold exceeded	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No
File System - Options	File System Mode Changed	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No
File System - Used Percentage	File System Threshold exceeded	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No
File System - Options - Clear	File System Mode Changed	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No
File System - Used Percentage	File System Threshold exceeded	Jan 11, 2017 2:03:26 AM	Jan 11, 2017 2:03:26 AM			View Template	No

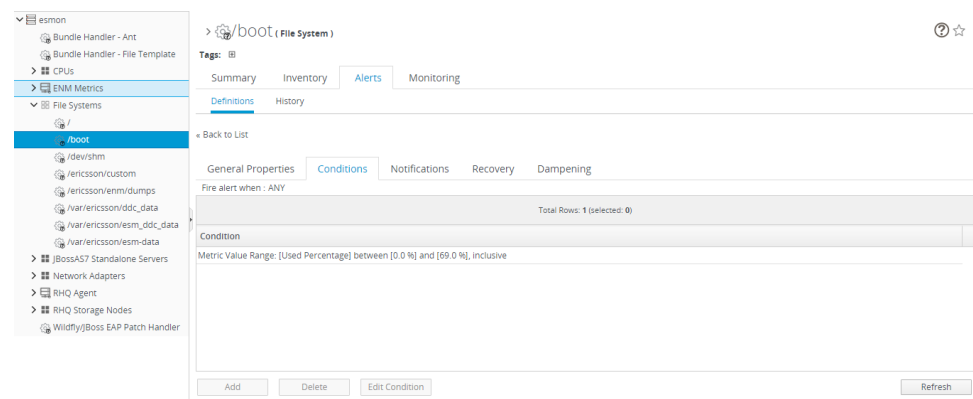
Result: The complete list of Alert Definitions for File System is displayed.

6. Select an **Alert Definition** based on the alert priority as shown in the **Priority** column.



Result: A page displaying general properties and conditions is displayed.

7. Click **Conditions**.



Result: The default conditions for the file system of that particular priority are displayed.

12.1.1 File System Used Percentage

The following table contains the default thresholds for File System templates.

Table 18 File System Used Percentage

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	File System - Used Percentage	File System Threshold exceeded	Used percentage $\geq 80\%$ and $\leq 90\%$	Low	FM Alert
2	File System - Used Percentage	File System Threshold exceeded	Used percentage $> 90\%$ and $< 95\%$	Medium	FM Alert
3	File System - Used Percentage	File System Threshold exceeded	Used percentage	High	FM Alert



S.No	Name	Description	Condition	Alert Priority	Notification Type
			>=95% and <=100%		
4	File System - Used Percentage - Clear	File System Threshold exceeded	Used percentage >=0% and <=79%	Low	FM Clear Alert

12.1.2 File System Mode Change

The following table contain details on file system modes.

Table 19 File System Mode

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	File System - Options	File System Mode Changed	When the File System Permissions are changed from ReadWrite to ReadOnly	Low	FM Alert
2	File System - Options - Clear	File System Mode Changed	When the File System Permissions are changed from ReadOnly to ReadWrite	Low	FM Clear Alert

12.2 View Linux Alert Thresholds

1. Click **Inventory**.
2. Click **Platforms**.
3. Select any Linux Platform from the **Platforms** list.
4. Click **Alerts**.



Summary Inventory Alerts Monitoring Events Operations Drift Content

Definitions History

Total Rows: 4 (selected: 0)

Name	Description	Creation Time	Modified Time	Enabled	Priority	Parent	Protected
Linux - Idle	CPU busy threshold exceeded	Jan 11, 2017 2:03:21 AM	Jan 11, 2017 2:03:21 AM	✔	🚩	View Template	No
Linux - Idle - Clear	CPU busy threshold exceeded	Jan 12, 2017 2:16:17 PM	Jan 12, 2017 2:16:17 PM	❌	🚩	View Template	No
Linux - Idle	CPU busy threshold exceeded	Jan 12, 2017 2:16:17 PM	Jan 12, 2017 2:16:17 PM	✔	🚩	View Template	No
Linux - Idle	CPU busy threshold exceeded	Jan 12, 2017 2:16:17 PM	Jan 12, 2017 2:16:17 PM	✔	🚩	View Template	No

Result: The list of Alert Definitions for Linux platforms is displayed.

- Select an **Alert Definition** based on the alert priority as shown in **Priority** column, a page displaying **General Properties** and **Conditions** is displayed.

« Back to List

General Properties Conditions Notifications Recovery Dampening

Name : Linux - Idle
 Description : CPU busy threshold exceeded
 Priority : 🚩 MEDIUM
 Enabled : Yes
 Protected : No

- Click **Conditions**.

« BACK TO LIST

General Properties Conditions Notifications Recovery Dampening

Fire alert when : ANY

Total Rows: 1 (selected: 0)

Condition
Metric Value Range: [Idle] between [5.0 %] and [10.0 %], exclusive



Result: The default thresholds for Linux of that particular priority are displayed.

12.2.1 Linux Default Alert Thresholds

The following table contains details of Linux default alert thresholds.

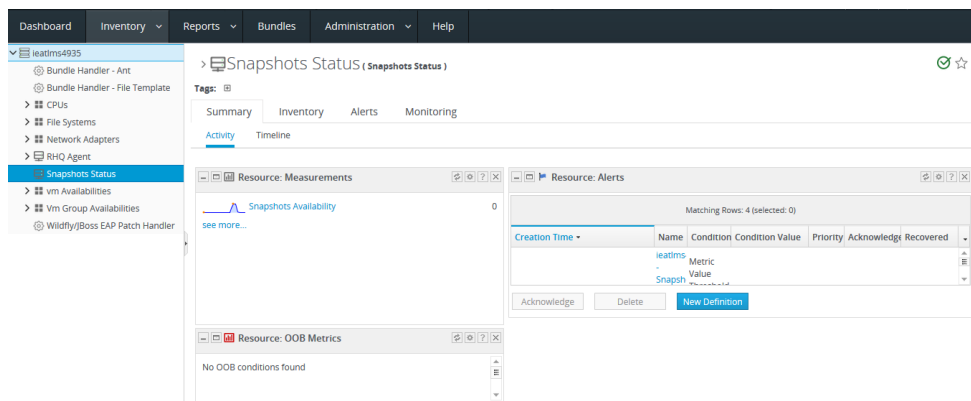
Table 20 Linux Default Alert Thresholds

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	Linux - Idle	CPU busy threshold exceeded	Idle >=10% and <=15%	Low	FM Alert
2	Linux - Idle	CPU busy threshold exceeded	Idle >5% and <10%	Medium	FM Alert
3	Linux - Idle	CPU busy threshold exceeded	Idle >=0% and <=5%	High	FM Alert
4	Linux - Idle - Clear	CPU busy threshold exceeded	Idle >15% to <=100%	Low	FM Clear Alert

12.3 View Snapshots Status Alert Thresholds

Steps

1. Click **Inventory**.
2. Click **Platform**.
3. Select **MS platform** from the platforms list.
4. Click **Snapshots Status**.





5. Click Alerts.

The screenshot shows the 'Snapshots Status (Snapshots Status)' page with the 'Alerts' tab selected. A table displays two alert definitions:

Name	Description	Creation Time	Modified Time	Enabled	Priority	Parent	Protected
leatims4935 - Snapshots Status - Snapshots Availability	Upgrade snapshots availability [with OPI]	Oct 26, 2017 6:49:26 AM	Nov 1, 2017 2:40:47 PM	<input checked="" type="checkbox"/>	■ HIGH		N/A
leatims4935 - Snapshots Status - Snapshots Availability - Clear	Upgrade snapshots availability [with OPI]	Oct 26, 2017 6:49:26 AM	Nov 1, 2017 2:40:47 PM	<input type="checkbox"/>	■ MEDIUM		N/A

The list Alert Definitions for Snapshots Status is displayed.

6. Select an Alert Definition based on the alert priority as shown in Priority column, a page displaying General Properties and Conditions are displayed.

The screenshot shows the 'Snapshots Status (Snapshots Status)' page with the 'Alerts' tab selected. The 'Alerts' sub-tab is active, displaying the following details for the selected alert definition:

- Name: leatims4935 - Snapshots Status - Snapshots Availability
- Description: Upgrade snapshots availability [with OPI]
- Priority: ■ HIGH
- Enabled: Yes

7. Click Conditions.

The screenshot shows the 'Snapshots Status (Snapshots Status)' page with the 'Alerts' tab selected. The 'Conditions' sub-tab is active, displaying the following details for the selected alert definition:

- Fire alert when: ANY
- Condition: Metric Value Threshold [Snapshots Availability > 0.0]

The default thresholds for Snapshots Status for the specified priority are displayed.



12.3.1 Snapshot Status Alert Threshold

This table provides details of snapshot status alert thresholds.

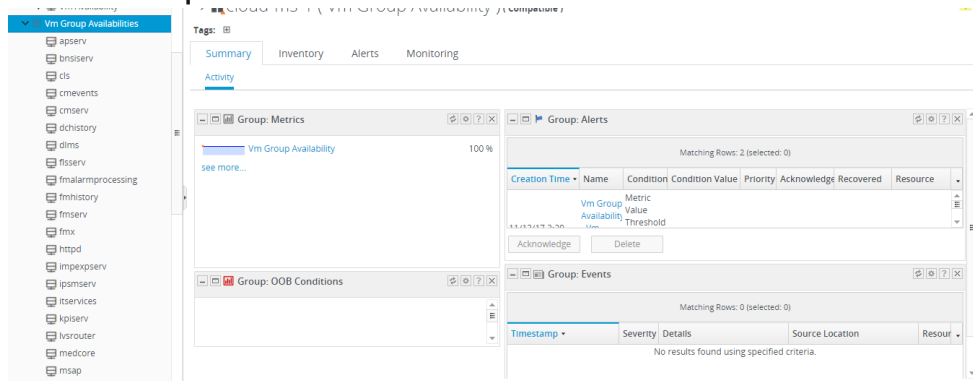
Table 21 Snapshots Status Alert Thresholds

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	Snapshots Availability	SAN snapshots older than 3 days available.	snapshots availability > 0	High	FM ALERT
2	Snapshots Availability	SAN snapshots older than 3 days available.	snapshots availability = 0	Low	FM Clear ALERT

12.4 View VM Group Availability Alert Thresholds

Steps

1. Click **Inventory**.
2. Click **Platform**
3. Select **MS platform** from the platforms list.
4. Click **Vm Group Availabilities**.



5. Click any VM.



6. Click Alerts > Definitions.

The screenshot shows the 'apsserv' alert definition page. The left sidebar lists various services, with 'apsserv' selected under 'Vm Group Availabilities'. The main content area shows the 'Definitions' tab with a table of alert definitions.

Name	Description	Creation Time	Modified Time	Enabled	Priority	Parent	Protected
Vm Group Availability - Vm Group Availability	Group Availability of Vm [with OPI]	Nov 13, 2017 11:48:49 AM	Nov 13, 2017 3:20:14 PM	Yes	High	View Template	No
Vm Group Availability - Vm Group Availability - Clear	Group Availability of Vm [with OPI]	Nov 13, 2017 11:48:49 AM	Nov 13, 2017 3:20:14 PM	No	High	View Template	No

Result: The list Alert Definitions for **VM Group Availability** are displayed.

7. Select an Alert Definition based on the alert priority as shown in **Priority** column, a page displaying **General Properties** and **Conditions** are displayed.

The screenshot shows the 'apsserv' alert definition page with the 'General Properties' tab selected. The properties are as follows:

- Name: Vm Group Availability - Vm Group Availability
- Description: Group Availability of Vm [with OPI]
- Priority: HIGH
- Enabled: Yes
- Protected: No

8. Click Conditions.

The screenshot shows the 'apsserv' alert definition page with the 'Conditions' tab selected. The condition is as follows:

- Fire alert when: ANY
- Condition: Metric Value Threshold [Vm Group Availability < 1.0 %]

Result: The default thresholds for **VM Group Availability** of a particular priority are displayed.



12.4.1 VM Group Availability Alert Thresholds

The following table contains details of VM group availability alert thresholds.

Table 22 VM Group Availability Alert Thresholds

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	VM Group Availability	Group availability of a VM type is less than 1%	VM Group Availability < 1.0%	High	FM ALERT
2	VM Group Availability	Group availability of a VM type is greater than 1%	VM Group Availability > 1.0%	Low	FM Clear ALERT

12.5 Edit Conditions

The user can edit the conditions at individual alert definition level, which is applicable for only file system or Linux platform and globally for all the file systems and Linux platform templates at administration.

1. Click **Administration**.
2. Click **Alert Definition Templates** under the **Configuration** section on the side menu.
3. Click **Edit** for either File System or Linux.



▼ Platforms			
Name ▲	Enabled Templates	Disabled Templates	Edit?
HP-UX	0	0	/
Java	0	0	/
Linux	3	1	/
Mac OS X	0	0	/
platform-a	0	0	/
▼ Platform Services			
Name ▲	Enabled Templates	Disabled Templates	Edit?
CPU	0	0	/
Directory	0	0	/
File System	4	2	/
File Template Bundle Handler	0	0	/
Hosts File	0	0	/
▼ Servers			

4. Select a template, and a page displaying general properties and conditions are displayed.
5. Edit the required conditions.



13 View Alerts for EMC Clariion or VNX Storage

ENM System Monitor (ESM) raises alarms when EMC-Clariion or VNX hardware fails. These templates are visible to all the users of ESM and no specific permissions are required to view them.

Prerequisites

- The user is logged on to Ericsson System Monitor.
- EMC Storage is imported.

Steps

1. Click **Inventory**.
2. Click **Platforms**.
3. Click **esmon**.
4. Click **EMC Storages**.
5. Click any **Hardware under EMC Storages**.
6. Click **Alerts**.

Name	Description	Creation Time	Modified Time	Enabled	Priority
EMC Storage - Fault Count - Clear	EMC Hardware has been faulted [with OPI]	May 20, 2017 7:37:02 PM	May 20, 2017 7:37:02 PM	⊘	🔔
EMC Storage - Fault Count	EMC Hardware has been faulted [with OPI]	May 20, 2017 7:37:02 PM	May 20, 2017 7:37:02 PM	⊙	🔔
EMC Storage - SPB Read Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:03 PM	May 24, 2017 12:28:03 PM	⊙	🔔
EMC Storage - SP Write Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:02 PM	May 24, 2017 12:28:02 PM	⊙	🔔
EMC Storage - SP Write Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:04 PM	May 24, 2017 12:28:04 PM	⊘	🔔
EMC Storage - SP Write Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:02 PM	May 24, 2017 12:28:02 PM	⊘	🔔
EMC Storage - SPA Write Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:03 PM	May 24, 2017 12:28:03 PM	⊙	🔔
EMC Storage - SPB Read Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:03 PM	May 24, 2017 12:28:03 PM	⊘	🔔
EMC Storage - SP Read Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:02 PM	May 24, 2017 12:28:02 PM	⊘	🔔
EMC Storage - SPB Write Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:04 PM	May 24, 2017 12:28:04 PM	⊘	🔔
EMC Storage - SP Read Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:02 PM	May 24, 2017 12:28:02 PM	⊙	🔔
EMC Storage - SPA Write Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:04 PM	May 24, 2017 12:28:04 PM	⊘	🔔
EMC Storage - SPA Read Cache State	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:03 PM	May 24, 2017 12:28:03 PM	⊙	🔔
EMC Storage - SPA Read Cache State - Clear	EMC Cache State not Enabled [with OPI]	May 24, 2017 12:28:03 PM	May 24, 2017 12:28:03 PM	⊘	🔔

— RELATED INFORMATION —

[13.1 Default Threshold for ENM Storage on page 77](#)



13.2 ESM EMC Metrics on page 78

13.1 Default Threshold for ENM Storage

The following table contains details of the default thresholds for EMC Storage.

Table 23 Default Threshold for ENM Storage

S.No	Name	Description	Condition	Alert Priority	Notification Type
1	EMC Storage - Fault Count	EMC Hardware is faulty	Fault Count > 0	CRITICAL	FM Alert
2	EMC Storage - Fault Count - Clear	EMC Hardware has been recovered	Fault Count = 0	LOW	FM Clear Alert
3	EMC Storage - SPA Read Cache State	EMC SPA Read Cache state is not enabled	Not Enabled	CRITICAL	FM Alert
4	EMC Storage - SPA Read Cache State - Clear	EMC SPA Read Cache state is enabled	Enabled	LOW	FM Clear Alert
5	EMC Storage - SPA Write Cache State	EMC SPA Write Cache state is not enabled	Not Enabled	CRITICAL	FM Alert
6	EMC Storage - SPA Write Cache State - Clear	EMC SPA Write Cache state is enabled	Enabled	LOW	FM Clear Alert
7	EMC Storage - SPB Read Cache State	EMC SPB Read Cache state is not enabled	Not Enabled	CRITICAL	FM Alert
8	EMC Storage - SPB Read Cache State - Clear	EMC SPB Read Cache state is enabled	Enabled	LOW	FM Clear Alert
9	EMC Storage - SPB Write Cache State	EMC SPB Write Cache state is not enabled	Not Enabled	CRITICAL	FM Alert
10	EMC Storage - SPB Write Cache State - Clear	EMC SPB Write Cache state is enabled	Enabled	LOW	FM Clear Alert



13.2 ESM EMC Metrics

This table contains details of the EMC Storage Metrics.

Table 24 EMC Storage Metrics

S.No	Metric Name	Description	Collection Interval
1	Fault Count	Count of faulted hardware components	15 minutes
2	SPA Read Cache State	Displays SPA Read Cache state as 0 (disabled) or 1 (enabled).	1 hour
3	SPA Write Cache State	Displays SPA Write Cache state as 0 (disabled) or 1 (enabled).	1 hour
4	SPB Read Cache State	Displays SPB Read Cache state as 0 (disabled) or 1 (enabled).	1 hour
5	SPB Write Cache State	Displays SPB Write Cache state as 0 (disabled) or 1 (enabled).	1 hour



Reference List

- [1] ENM Identity and Access Management System Administrator Guide, 2/1543-AOM 901 151-1
- [2] *ENM Monitoring System Administrator Guide*, 1/1543-AOM 901 151-2
- [3] *ENM Configuration System Administrator Guide* 1/1543-AOM 901 151-1
- [4] *ENM Performance Management System Administrator Guide* 1/1543-AOM 901 151-3