OpManager

USER GUIDE

Table of Contents

ManageEngine OpManager - Network Monitoring Software

With the growing need for the network monitoring software in the IT industry, OpManager has been built to satisfy the needs of network administrators by monitoring servers, routers, switches, firewalls, printers, critical services and applications from a single console.

Network Monitoring Software

ManageEngine OpManager is a comprehensive network monitoring software that provides the network administrators with an integrated console for managing routers, firewalls, servers, switches, and printers. OpManager offers extensive fault management and performance management functionality. It provides handy but powerful Customizable Dashboards and CCTV views that display the immediate status of your devices, at-a-glance reports, business views etc. OpManager also provides a lot of out-of-the-box graphs and reports, which give a wealth of information to the network administrators about the health of their networks, servers and applications.

OpManager's network monitoring functionality includes the following:

Network Monitoring: OpManager discovers switches, routers and firewalls in the network during the network discovery automatically and monitors the critical parameters such as the traffic rate, error and discards rate, buffer hits and misses and so on. You can get the availability report of each port and interface. Using the Switch Port Mapper tool, you can get the list of devices connected to each port of the switch. You can also create your own views and draw the diagram to virtually represent your network and get the availability of the interfaces visually.

Server Monitoring: OpManager allows you to classify devices as servers and desktops. This facilitates separating critical servers from end-user workstations and allows for more meaningful management. You can manage Windows Event Logs and Windows Services.

Cisco IPSLA Monitoring: OpManager allows you to monitor the performance of your VoIP networks with the Cisco IPSLA monitor. The Cisco IPSLA monitor is add-on feature and monitors the various parameter like Latency, Jitter, MoS etc.

WAN Monitoring: OpManager provides complete solutions for monitoring your WAN links. It checks for RTT, Latency and availability between the WAN links. The WAN monitor comes as an add-on feature.

VMware/Hyper-V Monitoring: OpManager out-of-the-box monitors VMware and Hyper-V servers. It monitors VMware servers via native APIs provided by VMware and Hyper-V servers via WMI. All the VMware and Hyper-V hosts and VMs are grouped under Virtualization tab.

Applications and Services Monitoring: OpManager discovers and actively monitors services and applications running in the servers. Out-of-the-box support is provided for services such as Web, HTTPS, FTP, IMAP, LDAP, Telnet, MySQL, MS-Exchange, SMTP, POP3, WebLogic, etc., and applications such as MSSQL, MS Exchange, Oracle and Lotus. Special add-ons are available for monitoring Exchange 2000/2003/2007 and Active Directory Services.

URL Monitoring: OpManager monitors your Web sites, both global URLs and URLs in the servers, and promptly notifies you when the host becomes unavailable.

Script Monitoring: OpManager monitors the output of the custom scripts you execute on the devices and raise alarm accordingly. OpManager parses the output of the custom scripts and verifies it with the configured threshold condition. If the threshold is violated an alarm is raised and the same is notified via the associated notification profile.

Fault Management: OpManager provides extensive solutions for monitoring Syslogs, Eventlogs and current Processes running on the devices. OpManager detects faults in the network through periodical status polling and generates color-coded alarms for the faults. OpManager can also be configured to notify the administrator about the fault detected in the network.

Performance Management: OpManager measures the performance of the network hardware and software, such as the bandwidth, memory, disk and CPU utilization, and service response time by collecting data at regular intervals. These data are provided in the form of reports and graphs to the administrators. The threshold limits can be configured to pro-actively monitor the critical parameters in the managed devices.

IT Automation Workflows: OpManager helps you automate repeated IT actions with Workflow. Workflow works on if-else based conditions which execute a set of actions when the given condition is satisfied, else executes another set of actions. However, you can also execute actions without any condition.

REST API: OpManager offers REST APIs for adding and fetching data from OpManager. Using these APIs, you can script the interactions or integrate 3rd party IT management/service desk software with OpManager.

Starting OpManager

After installation, all the OpManager-related files will be available under the directory that you choose to install OpManager. This is referred to as *OpManager Home* directory.

- Starting OpManager on Windows
- Starting OpManager on Linux
- Connecting the Web Client

On Windows Machines

If you have chosen to install OpManager as Windows service, you will be prompted to start the service after successful installation. The Web Client is invoked automatically on installing as a Service. Enter the log-on details. The default user name and password is 'admin' and 'admin' respectively.

To later start OpManager as a Windows Service, follow the steps below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Under **Administrative Tools**, select **Services**.
3. In the details pane, right-click **ManageEngine OpManager** and click **Start**.

To stop the ManageEngine OpManager service, right-click the **ManageEngine OpManager** service in the Services window and click **Stop**.

On Windows machines, an icon is displayed on the system tray to manage the application. You can start the client, start the server, and shut down the server using this icon.

On Linux Machines

1. Log in as '**root**' user.
2. Execute the **StartOpManagerServer.sh** file present in the *<OpManager Home>/bin* directory.

To stop OpManager running on a linux machine, execute the **ShutDownOpManager.sh** file present in the *<OpManager Home>/bin* directory.

Type the **User Name** and **Password** in the Shut Down OpManager window and press Enter.

Connecting the Web Client

1. Open a JavaScript-enabled Web browser such as Internet Explorer or Mozilla Firefox.
2. Type http://<**host_name**>:<**port_number**> in the address bar and press Enter. Here, <**host_name**> is the name of the machine in which OpManager is running and <**port_number**> is the port that you have chosen to run OpManager Web Server during installation.

   [Note: If you have enabled SSL, connect as https:///<**host_name**>:<**port_number**> in the address bar and press Enter.]
3. Type the **User Name** and **Password** and click **Login**. The default user name and password are 'admin' and 'admin' respectively.

Alternatively, if the OpManager server is running on Windows machines, you can start the Web client using
Start > Programs > ManageEngine OpManager > OpManager Web Client.

[OR]

Right-click the tray icon and select **Start Client** option.

From OpManager build 7010 onwards we provide SSL support for the webclient. Click here to enable SSL.

Enabling SSL in OpManager

Steps to enable SSL for OpManager build 8050 and above

In build 8050 we have remove Apache from OpManager. Follow the steps given below to enable SSL:

1. Open a command prompt (Run-> cmd) and change directory to /opmanager/bin.
2. Execute the following command

   ssl_gen.bat -f Enable

You have successfully enabled self signed SSL certificate for OpManager. Now you can access OpManager web client in the same port number with **https://**.

Steps to disable SSL:

1. Open a command prompt (Run-> cmd) and change directory to /opmanager/bin.
2. Execute the following command

   ssl_gen.bat Disable

This will disable SSL for OpManager. The web client can be accessed in the same port number with **http://**.

Steps to enable SSL for OpManager builds older than 8050 (Apache has been removed in build 8050)

1. Stop OpManager service.
2. Ensure service window is closed.
3. Open a command prompt and change directory to opmanagerbin.
4. Execute the script OpManagerService.bat with **-r** option as shown below:

   OpManagerService.bat -r

   This removes the Service entry.

5. From the command prompt, with opmanagerbin as the current directory, execute the script **ssl_gen.bat**. This creates the SSL Certificate.
6. Now, execute the OpManagerService.bat script once again, but with the argument as **-i** as shown below. This recreates the OpManager Service.

   OpManagerService.bat -i

7. Restart OpManager Service and connect as https://<opmanager host name or IP address>:<port number>. For instance, if the host name is OpM-Server and the port is 80, you will connect as

   https://OpM-Server:80

The WebClient is now SSL-enabled.

Steps to enable SSL for NetFlow plug-in

If you have also installed the NetFLow plug-in, then follow steps given below.

1. Ensure that SSL has already been enabled in OpManager.
2. Stop the OpManager Service.
3. Download and unzip the NetFlow_ssl.zip under opmanager folder.
4. Run the ssl_gen.bat present under opmanagerNetFlowbin.
5. This will create NetFlow.truststore and server.keystore under opmanagerNetFlowserverdefaultconfssl folder.

6. Start the OpManager service.

The NetFlow plug-in is also now SSL-enabled.

Steps to enable third-party SSL in OpManager

1. Open a command prompt (Run-> cmd) and change directory to /opmanager.
2. **Generate a Keystore file.** Execute the following command and provide requested details to create OpManager.truststore file under conf folder.
   >jrebinkeytool.exe -v -genkey -keyalg RSA -keystore confOpManager.truststore -alias opmanager (Press Enter)
   Enter keystore password:(Enter a password for this keystore. atleast 6 characters long. Press Enter)
   What is your first and last name?
   [Unknown]: (Enter the Server's name in which OpManager is running. It must be a FQDN [Fully Qualified Domain Name] Ex.: opmserver.manageengine.com. Press Enter.)
   What is the name of your organizational unit?
   [Unknown]: (Name of your Organization Unit. Ex: SYSADMIN. Press Enter.)
   What is the name of your organization?
   [Unknown]: (Your Organization Name. Ex:Zoho Corp. Press Enter.)
   What is the name of your City or Locality?
   [Unknown]: (Your city name. Ex:Pleasanton. Press Enter.)
   What is the name of your State or Province?
   [Unknown]: (Your state name. Ex:California. Press Enter.)
   What is the two-letter country code for this unit?
   [Unknown]: (Your country's two letter code. Ex:US. Press Enter.)
   Is CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US correct?
   [no]: (Check the details and if it is correct type yes and press enter. If else just press Enter to modify)
   Generating 1,024 bit RSA key pair and self-signed certificate (MD5WithRSA)
   for CN=opmserver.manageengine.com, OU=SYSADMIN, O=Zoho Corp, L=Pleasanton, ST=California, C=US
   Enter key password for <opmanager>
   (RETURN if same as keystore password): (Just press enter. For tomcat both keystore password and key [alias] password must be the same)
   [Storing confOpManager.truststore]
3. **Generating CSR File** (Certificate Signing Request). Execute the following commands to create opmssl.csr file under conf folder:
   >jrebinkeytool.exe -v -certreq -file confopmssl.csr -keystore confOpManager.truststore -alias opmanager
   Enter keystore password: (Enter the password for the keystore file)
   Certification request stored in file <confopmssl.csr>
   Submit this to your CA
4. **Get certificates from CA** (Certification Authority):
   Contact a CA like Verisign, Equifax, with the csr file generated in the previous step to get ssl certificate. Mostly you have to copy and paste the content of the csr file in a text area of their website. After verifying your request, mostly they will sent you the certificate content through mail. Copy and paste the content in a text editor and save it as "ServerCert.cer" under OpManager_Homeconf folder. Be cautious that while doing copy-paste, no extra space added at the end of lines.
5. **Import root and intermediate certificates:**
   Before importing our certificate, we have to import the CA's root and intermediate certificates into the keystore file we generated at the second step. While mailing you the certificate, CA's will mention the link to their root and intermediate certificates. Save them under conf directory in the name "CARoot.cer" and "CAIntermediate.cer" respectively. Some CAs may

have two or more intermediate certificates. Refer their document clearly before importing.

To import root certificate:

>jrebinkeytool.exe -import -trustcacerts -file confCARoot.cer -keystore confOpManager.truststore -alias CARootCert

Enter keystore password: (Enter the keystore password)

(Root Certificate's information will be printed)

Trust this certificate? [no]: (type yes and press enter if it is the certificate of your CA)

Certificate was added to keystore

To import intermediate certificate:

>jrebinkeytool.exe -import -trustcacerts -file confCAIntermediate.cer -keystore confOpManager.truststore -alias CAInterCert

Enter keystore password: (Enter the keystore password)

Certificate was added to keystore

6. **Import Server's Certificate.** Execute the following command to add the certificate received from CA to the keystore file:
   >jrebinkeytool.exe -import -trustcacerts -file confServerCert.cer -keystore confOpManager.truststore -alias opmanager
   Enter keystore password: (Enter the keystore password)
   Certificate reply was installed in keystore
7. **Configure Tomcat:**
   1. **Open "ssl_server.xml" file (under OpManager_Hometomcatconfbackup) in a text editor.**
   2. **Search for term "keystoreFile". It will be an attribute for connector tag. Set the value as "WEBNMS_ROOT_DIR/conf/OpManager.truststore".**
   3. **Change the value for "keystorePass" attribute with your keystore file password.**
8. **Modify conf file:**
   1. Open "OpManagerStartUp.properties" file (under OpManager_Homeconf) in a text editor.
   2. Set the value of the parameter "https" as "Enable".
9. Start OpManager server. Connect client with https. Ex:https://opmserver.manageengine.com:80

Note:

If you are already having a certificate for this server and that certificate was requested by the keystore file generated using Java keytool, you may use it for SSL configuration. Just copy and paste the keystore file under OpManager_Homeconf and rename it to “OpManager.truststore” and follow the steps from 5.

Registering OpManager

You can register OpManager by applying the license file that you receive from AdventNet. To apply the license, follow the steps given below:

1. Click **Register** at the top right corner of the client page.
2. Click **Browse** and choose the license file from the location it is saved.
3. Click the **Register** button to apply the license file and close.

Should you encounter any errors when applying the license, contact Support with the license error code.

Configuring Failover Support for OpManager

Failover or redundancy support for OpManager is necessary to achieve uninterrupted service. It becomes cumbersome if the OpManger DB crashes or loses its network connectivity and not monitoring your network. Though regular backups help you recover from DB crashes, but it takes time for OpManger to resume its service. However, in the mean time your network will be left unmonitored and some other critical devices such as routers, mail servers etc. may go down and affect your business. Implementing a redundancy system helps you to overcome such failures.

Failover support requires you to configure OpManager Secondary or Standby server and keep monitoring the OpManager Primary server. Incase the Primary server fails the Standby server automatically starts monitoring the network. The transition is so quick and smooth that the end user does not feel the impact of the failure of the Primary server or the subsequent taking over by Standby. In parallely the Standby server triggers an email alert (email ID entered configured in the mail server settings) about the Primary's failure. Once the Primary server is restored back to operation the Standby server automatically goes back to standby mode.

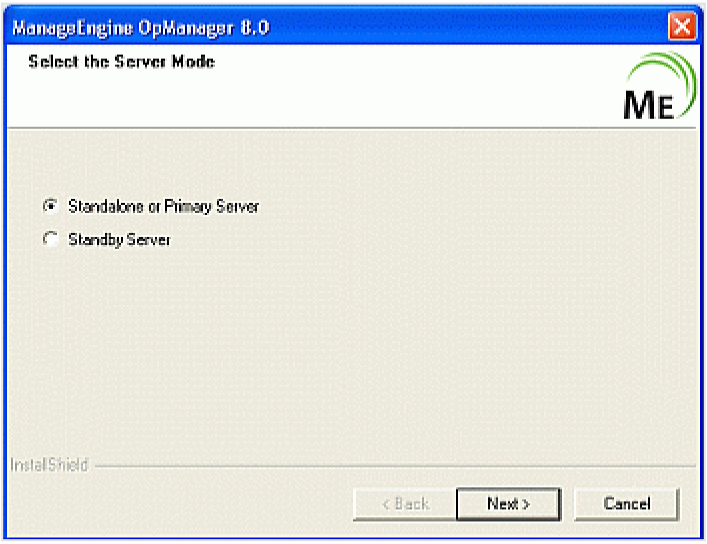
Working Mechanism

The Primary server updates its presence with a symbolic count in the BEFailover table at a specified interval known as the HEART_BEAT_INTERVAL. With every update the count gets incremented. This count is known as LASTCOUNT. Similarly the standby server also updates the its presence by updating the LASTCOUNT in the BEFailover table.

When the Primary server fails, it fails to update the LASTCOUNT. The Standby server keeps monitoring the Primary's LASTCOUNT at a specified periodic interval known as FAIL_OVER_INTERVAL. By default the FAIL_OVER_INTERVAL value is 60 seconds. If required you can modify it in the Failover.xml file (<OpManager_Standby_home>\conf). Supposing, you have specified FAIL_OVER_INTERVAL as 50 seconds, the standby will monitor the Primary's LASTCOUNT for every 50 seconds. Every time, when the Standby server looks up the LASTCOUNT, it compares the previous and present counts. When the Primary server fails to update the LASTCOUNT, consecutive counts will be the same and the Standby assumes that the Primary server has failed and starts monitoring the network.

Installing the Primary Server

If you are already running OpManager, first upgrade to build 7260 before applying build 8000. If you installing OpManager for the first time directly install build 8000. While installing OpManger (build 8000) on the Primary server, select as Primary server in the installation wizard and complete the installation process. Start the Primary server.



ManageEngine OpManager 8.0

Select the Server Mode

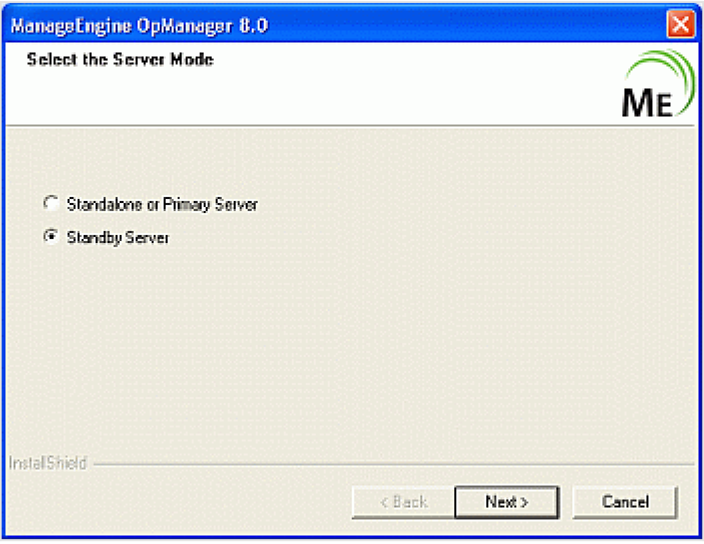
● Standalone or Primary Server

○ Standby Server

Installing the Standby Server

While installing OpManager on the standby server,

1. Select as Standby server mode in the installation wizard.



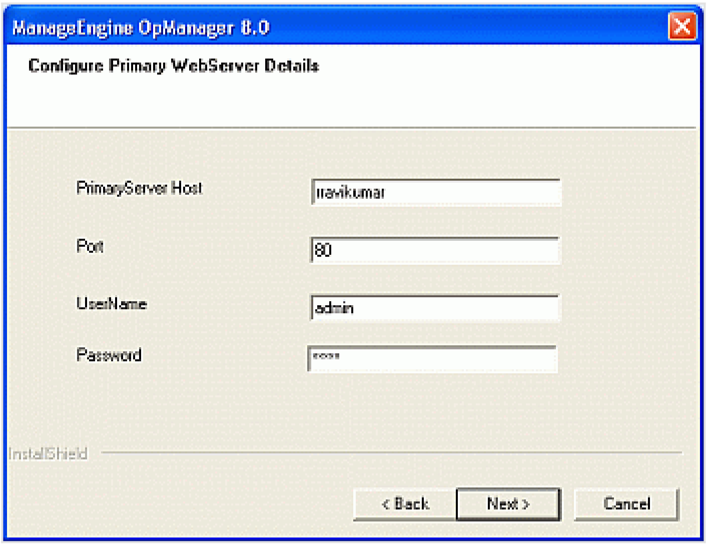
ManageEngine OpManager 8.0

Select the Server Mode

○ Standalone or Primary Server

● Standby Server

2. Enter the Primary webserver host, port and login details and complete the installation. Do not start the Standby server.



ManageEngine OpManager 8.0

Configure Primary WebServer Details

PrimaryServer Host: ravikumar

Port: 80

UserName: admin

Password: ****

Note: The Date and Time settings of the Primary and the Standby should be same.

Configuring Failover:

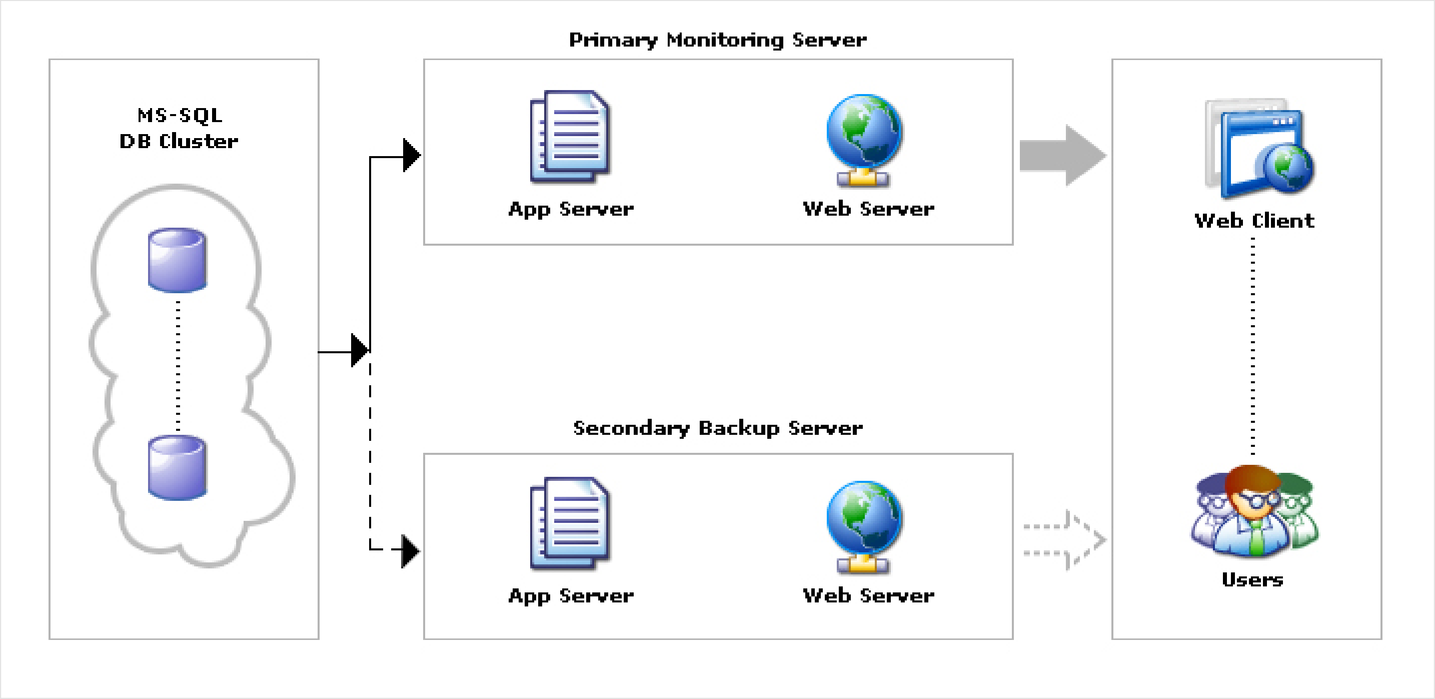
The procedures for configuring failover support varies according to the following cases (backend DB used):

- Using MSSQL

Using MSSQL as the backend DB

If you are running OpManager with MSSQL as the backend DB, then implement clustering. Clustering refers to an array of databases in which the data are stored and have a single virtual IP. If any of the DB in the cluster environment fails the other DBs have the data thereby providing high availability of data. The Primary server sends all its data to a virtual IP and the data gets stored in multiple locations. The Standby server that takes control over the network in case the primary fails, then the standby server also sends the data to the same virtual IP.

For configuring MSSQL server clustering visit the below link published by Microsoft.
http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/failclus.mspx#EDAAC



For MSSQL, the Standby OpManager server can be started once the installation is completed, provided you have already configured MSSQL clustering for Primary server.

Once the Primary server fails, the Standby server assumes itself as the Primary server and starts monitoring the network. Once the Primary server is up, the Standby server goes back to its standby mode and monitors the Primary server.

Migrating Database

OpManager supports MySQL and MSSQL as the backend database. At a later time, you can choose to migrate from one database to another. Here are the steps:

Migrating from MySQL to MSSQL

Prerequisites

- The Build Number of OpManager must be 6000 or higher.
- MSSQL database must be installed as this is not bundled with OpManager.

Steps to migrate are,

1. Stop OpManager again and take a backup of the data using BackupDB.bat
   present under /bin/backup directory .
2. Select Start --> Programs --> ManageEngine OpManager --> DB Manager --> DB Configuration.
3. A DB Configuration window pops up. Select MSSQL option.
4. Configure the following information:
   1. DB Host : The name or the IP address of the machine where MSSQL is installed.
   2. Port: The port number in which OpManager must connect with the database. Default is 1433.
   3. User Name and Password: The user name and password with which OpManager needs to connect to the database.
   4. Driver Jars: Specify the path of the Database driver
   5. Click OK.
5. Restore the data using RestoreDB.bat present in /bin/backup directory
   and restart OpManager.

Refer to our online knowledgebase article to configure Microsoft MSSQL JDBC driver.

Data Backup and Restoration

Periodically backing up the database is very essential, as it helps you restore OpManager service back during planned maintenance as well as unplanned mishaps. OpManager database contains two types of data:

Performance data: This is the data gathered by OpManager by periodically polling or querying the resources on a monitored device to determine its performance. This includes resources like CPU, Memory, Response time, Traffic etc.

Configuration data: There are quite a few configurations an administrator effects in OpManager for easy management and monitoring. The configurations include user settings, details of discovered devices, custom monitors, threshold settings, notification profiles, etc. Most configuration data is persisted in the database while a few configurations are written in conf files. So when you backup configuration data, you must take care to back up the ones you need.

- Backup & restoration steps for OpManager build 9450 and above
- Backup & restoration steps for OpManager build 9410 and below

Backup & restoration steps for OpManager build 9450 and above

Backup

Following table lists the backup utilities bundled with OpManager and their purpose. Make sure you use the one that fits your backup need:

S.No	Utility	Path	Database	Purpose
1	**BackupDB_Mysql.bat/sh** Arguments: mode, destination, exclude, threads **mode*:** Backs up either both performance and configuration data or configuration data alone possible values: all, configdata ('all' backs up both performance and configuration data while 'configdata' backs up configuration data alone) **destination**: This option is used to store the backup file in different location. By default it will be stored in <OpManager Home/backup> directory. **exclude:** Allows you to exclude netflow and ncm plugin data while taking backup possible values: ncm, netflow **threads:** Increasing the number of threads will increase the backup speed. Default thread count is 10, but you can increase up to 15. Examples: • BackupDB_Mysql.bat -mode all -exclude ncm • BackupDB_Mysql.bat -mode configdata -threads 12 -destination c:\manageengine *- Mandatory field	*OpManager Home>/bin /backup*	MySQL	This utility does a backup of the complete database, viz., performance and configuration data. If you are using MySQL bundled with OpManager and assuming that you will not switch to MSSQL database when restoring the backed-up data.

2	**BackupDB_Postgres.bat/sh** Arguments: mode, destination, exclude, threads **mode*:** Backs up either both performance and configuration data or configuration data alone possible values: all, configdata ('all' backs up both performance and configuration data while 'configdata' backs up configuration data alone) **destination:** This option is used to store the backup file in different location. By default it will be stored in <OpManager Home/backup> directory. **exclude:** Allows you to exclude netflow and ncm plugin data while taking backup possible values: ncm, netflow **threads:** Increasing the number of threads will increase the backup speed. Default thread count is 10, but you can extend up to 15. Examples: • BackupDB_Postgres.bat -mode all -exclude netflow • BackupDB_Postgres.bat -mode configdata -threads 12 -destination c:\manageengine *- Mandatory field	*-do-*	PostrgreSQL	This utility does a backup of the complete database, viz., performance and configuration data. If you are using PostgreSQL bundled with OpManager and assuming that you will not switch to MSSQL database when restoring the backed-up data.
3	**CrossDBBackup.bat/sh** Arguments: mode, targetdb, destination, exclude, threads **mode*:** backs up performance data or configuration data or configuration files or all the aforesaid. possible values: all, configdata, configfiles ('all' backs up both performance and configuration data while 'configdata' backs up configuration data alone. When you backup the DB using Microsoft SQL Enterprise, it does a backup of only the database and ignores the configuration files which are required to run OpManager properly. To backup those configuration files, use the 'configfiles'.) **targetdb*:** The target database that you are going to restore the backup. possible values: mysql, mssql, pgsql **destination:** This option is used to store the backup file in different location. By default it will be stored in <OpManager Home/backup> directory. **exclude:** Allows you to exclude netflow and ncm plugin data while taking backup possible values: ncm, netflow **threads:** Increasing the number of threads will increase the backup speed. Default thread count is 10, but you can extend up to 15. Examples: • CrossDBBackup.bat -mode all -exclude ncm -targetdb pgsql • CrossDBBackup.bat -mode configdata -threads 12 -destination c:\manageengine -targetdb mssql • CrossDBBackup.bat -mode all -exclude netflow -targetdb mssql *- Mandatory field	*-do-*	MSSQL/ MySQL/ PostgreSQL	This utility does a backup of the complete database, viz., performance and configuration data. Use this tool if you are migrating the database across MSSQL, MySQL & PostrgreSQL.

Restoration

To restore the backed up data,

1. Go to *<OpManager Home>/bin/backup* directory
2. Execute **RestoreDB.bat/sh** with the backup file name as argument. See example below:

   C:\<OpManager Home>\bin\backup>RestoreDB.bat BackUp_APR3_2009_17_43_38_8100.zip

While restoring the backup, the tables that are dropped or retained varies according to the backup file restored:

Options:

- exclude: Used to skip restore data for ncm and netflow plugin.
  Possible values : ncm, netflow
- threads - Increasing the number of threads will increase the restore speed.
  Value should be less than 15. default 10.

Examples :

- RestoreDB.bat BackUp_APR3_2009_17_43_38_8100.zip
- RestoreDB.bat BackUp_APR3_2009_17_43_38_8100.zip -exclude ncm,netflow

Note: If you are restoring from PostrgeSQL or MySQL database to MSSQL, download and install SQL native client (refer the installation video) and follow the steps given below:

1. Ensure that the files bcp.exe and bcp.rll files are present under /opmanager home folder. You will find these files in MSSQL installation setup.
2. If the MSSQL server is installed on a 64-bit OS, and OpManager is installed on 32-bit server, the bcp.exe and bcp.rll copied from the MSSQL server will not work on the OpManager machine. You'll need a 32-bit bcp.exe and bcp.rll.

Backup & restoration steps for OpManager build 9410 and below

Backup

Following table lists the backup utilities bundled with OpManager and their purpose. Make sure you use the one that fits your backup need:

S.No	Utility	Path	Database	Purpose
1	**BackupDB_Mysql.bat/sh**	*OpManager Home>/bin/backup*	MySQL	This utility does a backup of the complete database, viz., performance and configuration data. If you are using MySQL bundled with OpManager and assuming that you will not switch to MSSQL database when restoring the backed-up data. Ensures a quick backup.
2	**BackupDB_Mysql_Config.bat/sh**	-do-	MySQL	Use this tool if you want to backup only the configuration data and not the performance data. This requirement arises when you decide that you want to drop all the performance data and start afresh in the same or new machine, but keep all the configurations alone intact. Ensures a quick backup.
3	**BackupDB.bat/sh**	-do-	MSSQL/MySQL	This utility does a backup of the complete database, viz., performance and configuration data. Use this tool if you are using MSSQL as the database. It can also be used for MySQL database besides BackupDB_Mysql.bat/sh, but might take a longer time to backup. Advantage of using this utility is that you can backup and restore from MySQL to MSSQL and vice versa.

4	**BackupDB_Config.bat/sh**	-do-	MSSQL/MySQL	Use this tool if the OpManager database is MSSQL and if you want to backup only the configuration data and not the performance data. This requirement arises when you decide that you want to drop all the performance data and start afresh in the same or new machine, but keep all the configurations alone intact.
5	**Microsoft SQL Enterprise Manager + BackupConfFiles.bat**	-do-	MSSQL	You can also use **Microsoft SQL Enterprise Manager** to backup the database. When you use this tool, make sure to backup the configuration files too using the **BackupConfFiles.bat** utility because the SQL Enterprise Manager does a backup of only the database and ignores the configuration files which are required to run OpManager properly.
6	**Using third party backup utility + BackupConfFiles.bat**	-do-	MSSQL/MySQL	When you use any third party backup utility, make sure to backup the configuration files too using the **BackupConfFiles.bat** utility because the SQL Enterprise Manager does a backup of only the database and ignores the configuration files which are required to run OpManager properly.

Name & Location of the backup files

The backup file created is of the format: <filename>_<date>_<time>_<build number>.zip

Example: BackUp_APR3_2009_17_43_38_8100.zip.

The backup files are stored under OpManager Home/backup directory. To store the backup file in another directory other than the default directory (<OpManager Home/backup>), follow the procedure below:

1. Open a command prompt.
2. From the command prompt, execute the backup script (that meets your requirement) with the path of the destination directory as argument as follows:

   ```
   <backup execution command> -destination <path of the destination directory>
   ```

   Example:

   ```
   BackupDB_Mysql.bat -destination D:\OpManager_backup
   ```

Restoration

To restore the backed up data,

1. Go to *<OpManager Home>/bin/backup* directory
2. Execute **RestoreDB.bat/sh** with the backup file name as argument. See example below:

   ```
   C:\<OpManager Home>\bin\backup>RestoreDB.bat BackUp_APR3_2009_17_43_38_8100.zip
   ```

While restoring the backup, the tables that are dropped or retained varies according to the backup file restored:

- **BackupDB.bat/sh:** During restoration, all the existing tables are dropped, new tables are created, and the data are restored.
- **BackupDB_Config.bat/sh:** During restoration, all the existing tables are dropped, new tables are created, and only the configuration data are restored.
- **BackupDB_Mysql.bat/sh:** During restoration, all the existing tables are dropped, new tables are created, and the data are restored.
- **BackupDB_Mysql_Config.bat/sh:** During restoration, all the existing tables are dropped, new tables are created, and only the configuration data are restored.
- **BackupConfFiles.bat/sh:** During restoration, no tables get dropped. Only the configurations files are restored.

Changing Ports in OpManager

You will be prompted to change Web Server port during installation. You can change it after installation.

The script for changing the Web Server port number, **ChangeWebServerPort** (in Windows this will be a *.bat* file and in Linux, *.sh* file) is available under the *<OpManager Home>/bin* directory.

The steps to change the port number are as follows:

1. Stop the OpManager server. If you are running OpManager as Windows service, stop the service.
2. Execute the script as follows:

   In Windows,

   ChangeWebServerPort <old_port_number> <new_port_number>

   In Linux,

   sh ChangeWebServerPort.sh <old_port_number> <new_port_number>

   Here, old_port_number is the port number you specified during installation and new_port_number is the one where you want to run the Web server.
3. Start the OpManager server.

Changing Other Ports

You can also change the port by editing the value of WEBSERVER_PORT=80 in the file /conf/Port.properties.

You can change the following ports too in this file if the default ports are occupied:

```
WEBCONTAINER_PORT=8009
NMS_BE_PORT=2000
WEBSERVER_PORT=80
TOMCAT_SHUTDOWNPORT=8005
RMI_PORT=1099
```

Configuring System Settings

The following system settings can be enabled/disabled by the users.

Benchmark Statistics: Data collected from the OpManager community is presented to the user for benchmarking their performance. Click on the community tab to know more.

Usage Statistics: We collect statistical data pertaining to quality, stability, and usability of the product from every installation with an intent to enhance the product quality. The collected data will be used as a whole during the analysis and we won't share this data with others. This feature is enabled by default. If you don't want your data to be collected, you can disable it any time.

Quick Links: Provides the list of frequently asked questions that will help you to know more about OpManager.

Show Ads: Displays the ads from ManageEngine in the OpManager login UI.

Logging: For quick troubleshooting of monitoring issues, you can now enable detailed logging for SNMP,WMI and CLI monitors and debug prints. This logs the relevant requests to devices and helps troubleshoot.

Date and Time Format Settings: Select the required format for the date and time displayed in OpManager web client.

What Should Be Monitored?

Active network monitoring is a must to gain accurate and real-time visibility of the health of your network. However frequent monitoring can become a huge strain on your network resources as it generates a lot of traffic on the network, especially in large networks.

We recommend monitoring only the critical devices on the network. This is a best practice adopted by the network administrators worldwide.

Following are the components of networks that are considered critical:

- WAN Infrastructure: Routers, WAN Switches, Firewall, etc.
- LAN Infrastructure: Switches, Hubs, and Printers.
- Servers, Services, and Applications: Application Servers, Database servers, Active Directory, Exchange Servers, Web servers, Mail servers, CRM Applications, etc.
- Host Resources: CPU, Memory, and Disk Utilization of critical devices.
- Critical Desktops and Workstations.

Monitoring Interval for a Device Category

OpManager allows you to set a common monitoring settings for all the devices under a specific category.

To do so, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Monitoring**, click **Monitoring Intervals**.
3. To enable monitoring for a category, select the check box under **Enable** corresponding to the category and type the monitoring interval in minutes, in the adjacent box.

   To disable monitoring a specific category, clear the respective check box.
4. Click **Save** to save the settings.

For instance, if you want to monitor servers every minute, ensure that the check box corresponding to **Servers** is selected and type 1 in the adjacent box.

How Frequently Should I Monitor?

The general practice is to monitor critical devices more frequently than non-critical devices.

Given below are the recommended monitoring intervals for small and medium-sized networks (up to 1000 devices):

- Routers and Critical Servers: 10 minutes
- Switches, Hubs, and Printers: 10 - 20 minutes
- Critical Services like Exchange, Active Directory: 10 - 20 minutes
- Desktops and Workstations: We recommend turning off monitoring for desktops and workstations to reduce the amount of network traffic generated by OpManager.
  This is done by removing selection for Desktop category in Admin > Monitoring Intervals. Alternatively, monitor them less frequently, say for every hour or 30 minutes.

  If there are a few critical workstations that you want to monitor, you can turn on monitoring for those devices individually.

Personalize WebClient

Change Password

You can change the WebClient login password. Click on the **Personalize** link in the WebClient and select the **Change Password** tab. Provide the current password and the new password. Retype new password to confirm. The next time you login, use the new password.

Select Skin

From the Personalize link, select the **Skin Selector** tab to select the required skin for the WebClient.

Configure Automatic Refresh

From the Personalize link, select the **Automatic Refresh** tab to set automatic page refresh at the selected interval. You can also set the session timeout interval here.

Add Credentials

OpManager accesses the remote devices using the protocols SNMP, CLI, or WMI. The credentials like the password/snmp community, port etc., may differ for different device types. Pre-configuring a set of credentials in OpManager helps applying them to multiple devices at a time, saving a lot of manual effort.

1.Go to Admin --> Credential Settings.

2.Click New in this screen

3.Configure the following parameters and click Add to add the credentials:

Credential Type: Select the relevant protocol.

> **SNMP v1/SNMPv2**: SNMPv1 and SNMPv2 are community based security models. Enter the Credential name and description. Configure the correct Read and Write community, and the SNMP Port.
>
> **SNMP v3**: SNMPv3 is a user based security model. It provides secure access to the devices by a combination authenticating and encrypting packets over the network. The security features provided in SNMPv3 are Message integrity, Authentication and Encryption. If you select SNMPv3 as the credential type, then configure the following parameters.
>
> 1. **Name**: Enter the name of the credential.
> 2. **Description**: Enter a brief description about the credential.
> 3. **User Name**: Enter the name of the user (principal) on behalf of whom the message is being exchanged.
> 4. **Context Name**: An SNMP context name or "context" in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under certain context by an SNMPv3 entity, then any management application can access that information by giving that context name. The "context name" is an octet string, which has at least one management information.
> 5. **SNMP Port**: Enter the SNMP port number.
> 6. **Authentication**: Select any of the authentication protocols either MD5 or SHA and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.
> 7. **Encryption**: Select any of the encryption protocols either DES or EAS-128 and enter the password. Note: Only after configuring Authentication it is possible to configure Encryption.
>
> **WMI**: If you select WMI as the protocol, configure the Domain Name, the user name, and the password. Example:- *TestDomainTestUser.* Also enter the credential name and description.
>
> **Telnet/SSH**: Enter the credential name and description. For Telnet/SSH, make sure you configure the correct login prompt, command prompt, and password prompt besides the user name and password to access the device.
>
> **VMware**: Provide the HTTPS Username and Password of the Host. Enter the HTTPS web service port number and timeout interval for the connection between the Host and OpManager server.

The SNMP credentials created is used during the initial discovery and classifications. OpManager uses these credentials to classify and add the devices into OpManager.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Associate a credential to several devices** and click Next.
3. All the available Credentials are listed. Select the Credential which you want to associate to your devices.
4. Select the devices to which you want to assign the credential from the column on the left and move them to the right.
5. Click Finish. The Credential is associated to the selected devices.

Rule Engine

Rule Engine helps you automate the activities such as adding monitors to a device or adding a device to a business view that you carryout after adding the devices to OpManager. This helps you start monitoring the devices straightaway as soon as you add them and avoid repetitive manual effort.

How does Rule Engine Work?

The Rule Engine is condition/criteria based. During discovery, devices that satisfy the condition/criteria are associated with the actions specified in the Rule Engine.

Steps to add a Rule Engine

1. Go to **Admin**-> **Rule Engine**-> **Add New**.
2. Enter a **Name** and **Description** for the Rule Engine.
3. Define the **Criteria** and select the Condition.

   Eg. Select Service Name as the Criteria and equals as the Condition, and enter the POP3Svc (POP3Svc is a MSExchange service. This is to verify whether the discovered device is an exchange server or not.)
4. Click **Add**. If required you can define multiple criteria, but have to select either AND or OR option.

   AND: Executes the action when all the defined criteria are satisfied.

   OR: Executes the actions when any one of the defined criteria is satisfied.
5. Define the actions

   Eg. Select Add Service Monitor as the action and select the requiredservice monitors (Exchange server related monitors are added to thedevices that satisy the POP3Svc condition.)
6. Click **Add**. If required you can define multiple actions as well.
7. Click **Save** to save the rule.

How to video:

Actions with Rule Engine

Following are the action that be done on a created rule engine

- Edit
- Copy As
- Enable/Disable
- Delete

Click the respective icons to carryout these actions on a Rule Engine.

Re-running a Rule

To re-run a rule on demand,

1. Select the rule that you want to re-run.
2. Click on the **Re-run** button.
3. Select the devices on which you want to execute the rule.
4. Click **OK**.

Discovering Networks Using OpManager

You can discover devices on a network by either specifying a range or the entire network

OpManager uses ICMP/Nmap to discover the devices on a network.

Discover a range

To discover devices from a selected range specify the start and end ip address and select the netmask for the devices to be discovered within that range.

1. Click the Admin tab.
2. Under Discovery, select Discover Devices.
3. Use IP Range: Select this option to specify the range.
4. Start IP: Specify the IP address of the device in the range from where OpManager should start discovery.
5. End IP: Specify the IP address till which OpManager should discover.
6. Netmask: Select the correct netmask.
7. Discovery Credentials: Select the configured Credentials to be used for discovery.
8. Advanced SNMP Settings: Click here to configure an increase SNMP timeout or SNMP retries.

Discover a complete network

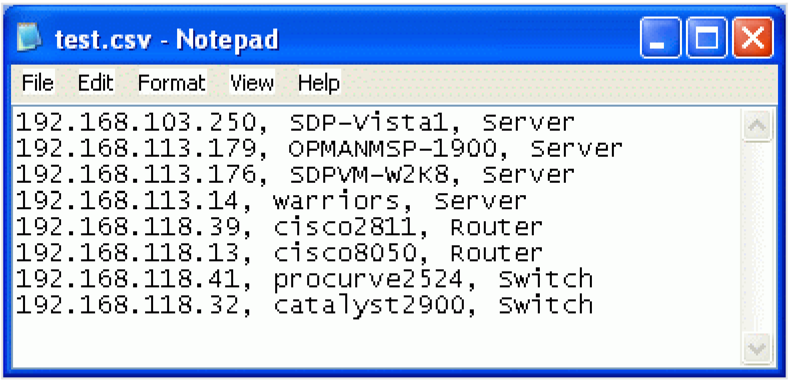
1. Use CIDR: Select this option to discover an entire network.
2. Network IP: Specify the Network IP to be discovered.
3. Credentials: Select the credentials and SNMP settings as mentioned above.
4. Click Discovery for the discovery to start.

OpManager supports discovering Hyper-V hosts and VMs using CIDR.

Discover by Importing from a file

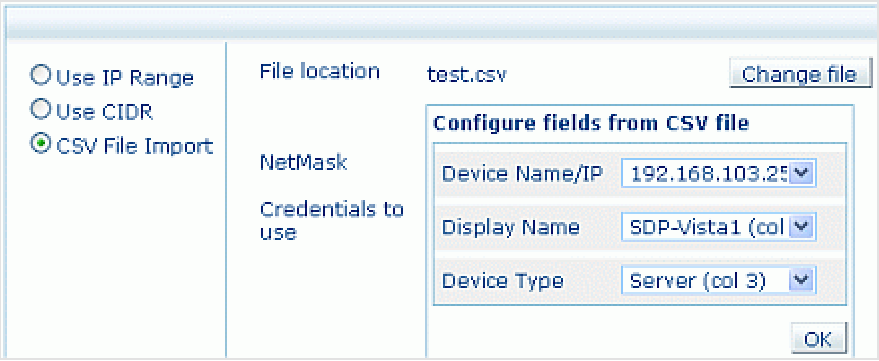
You can import a set of IP addresses for discovery from a csv file.

1. Create a csv file (as shown below) with the details of name/ipaddress of the device, displayname and device type.



```
192.168.103.250, SDP-Vista1, Server
192.168.113.179, OPMANMSP-1900, Server
192.168.113.176, SDPVM-W2K8, Server
192.168.113.14, warriors, Server
192.168.118.39, cisco2811, Router
192.168.118.13, cisco8050, Router
192.168.118.41, procurve2524, Switch
192.168.118.32, catalyst2900, Switch
```

2. Browse and select the CSV file from which you want the devices discovered and imported.
3. Select the Device Name/IP, Display Name and Device Type columns in the CSV file and click OK.



○ Use IP Range
○ Use CIDR
● CSV File Import

File location test.csv

NetMask

Credentials to use

Configure fields from CSV file

Device Name/IP 192.168.103.25

Display Name SDP-Vista1 (col

Device Type Server (col 3)

4. Provide the correct netmask.

Import the Devices into OpManager

All the discovered devices are listed category-wise.

1. Click Import Devices to add all the devices for monitoring.
2. Click Finish once the devices are added.

Discover Individual Devices

You might have added more devices to your network and may therefore need to forcefully discover these devices. You can discover such devices on demand by following the steps below:

1. Click the Admin tab.
2. Under Discovery, select Add Device .
3. Type either the IP Address or the Device Name of the device to be discovered.
4. Enter the correct Netmask/Network IP. Example: **IPv4-**255.255.255.0, **IPv6-**fe80::b343:567e:c254:0
5. Select the discovery credentials.
6. Click Add Device to start discover

The device is discovered and classified properly.
Alternatively, you can also add devices to a specific category directly.

1. Go to the required map view, say Servers Map or Routers map.
2. Click the Add Server/Router/... etc option on top of the map to discover and classify the device into that particular category.

Note: If you are unable to add the device or if does not show up in the map in which you are looking for, try pinging the device from the OpManager machine and check for response. Search the device using the Device Search box on the top right corner in the WebClient.

Layer 2 Mapping

OpManager renders the logical network topology diagram once you discover the networks and network devices. For a better visualization of the physical network connectivity in real networks and the consequences of a failure of a device, network topology map comes handy. To enable automatic layer 2 mapping, post discovery, you will need to specify the seed file so that layer 2 mapping is automatically done. OpManager purely relies on SNMP to represent the connectivity of nodes and links in the network. This document explains the following:

- What is a seed device
- Configuring seed device in OpManager
- Saving the map as a Business View
- Exporting a map to Visio

What is a seed device?

A seed device is the core switch in your network. The switch must have SNMP-enabled so that OpManager is able to query the device and draw the links automatically, showing the connectivity of all the devices on your network. As changes happen to the networks frequently, OpManager allows you to configure an interval (in days) to re-draw the map. For instance, if a change happens once in a week, you can configure OpManager to re-draw the map every seven days.

Configuring the seed device

1. From the OpManager dashboard, select Maps --> Network Maps link (mouse-over the Maps tab to see the links to all the maps).
2. In the Networks Map, select Actions --> Settings menu to your right.
3. You will find a combo-box to select the seed device. Select the core switch from the list.
4. Select the topology layout from the layout combo-box.
5. Specify the interval (in days) at which the map must be re-drawn in the Sampling Interval field and click Submit.

The map is generated. You can change the layout by selecting the type as Radial Tree, Balloon Tree, Node Link or Custom option for the Layout combo-box on top of the network map. You can also export the map to Visio, or even save it as a business view in OpManager.

Saving the Layer 2 Map as a Business View

1. In the Networks Map, select the menu Actions --> Save As.
2. Configure a name for the view in the dialog that pops up.

It is saved as a business view which you can assign to a user based on his role. You can access this business view from the Maps tab.

Exporting to Visio

Prerequisites

Make sure you have Microsoft Visio 2007. Visio can be installed on any of your Windows devices and it need not be on the same server as OpManager. Ensure that you are able to access OpManager Weblcient from the machine where Visio is installed.

Installation

1. Download OpManager Add-in for Microsoft Visio from here.
2. Unzip the add-in download and extract the file ***ManageEngineOpManagerMicrosoftVisioAddin.msi.***
3. Double-click the ***msi*** file to install the Add-in.
4. After successful installation, launch Visio and look for OpManager menu in the menubar. The add-in has installed properly if you find the menu!

Exporting Views from OpManager

1. Access OpManager webclient from the machine where MS Visio 2007 is installed.
2. You can export the map to Visio from the Network Maps link using Actions --> Export to Visio menu.
3. You can also export it from the business views using the Export to Visio button on top of the corresponding business view.
4. On exporting, you will be prompted to save the corresponding XML file with the name TopoMap.xml. Save the map in the

desired location on that machine.

Loading the exported maps in Visio

1. From the Visio GUI, access OpManager --> Load Map menu from the menubar.
2. Browse and select the TopoMap.xml (you can rename the xml after you save it on the machine). The exported map will be loaded in Visio.
3. Make the desired changes and save. You can save the diagram as a vsd file or in standard Visio formats.

Managing and Unmanaging a Device

By default, OpManager manages all the discovered devices. However, there might be some known devices that are under maintenance and hence cannot respond to status polls sent by OpManager. These devices can be set to unmanaged status to avoid unnecessary polling. Once maintenance gets over, they can be set to managed status.

To unmanage a device

1. Go to the device snapshot page.
2. Under **Actions**, select **Unmanage**.

This stops the status polling and data collection for the device and changes the device status icon to gray .

To start managing an unmanaged device

1. Go to the device snapshot page.
2. Under **Actions**, select **Manage**.

This resumes the status polling and data collection for the device. The status icon shows the current status of the device.

To manage or unmanage many devices at a time, you can use Quick Configuration wizard of OpManager. To do so, follow the steps below:

1. In the **Admin** tab, under **Tools**, click Quick Configuration Wizard.
2. Select **Manage/Unmanage devices** and click **Next**.
3. Select the category from which you want to unmanage.
4. To stop managing the devices, move them to the list in the right. To start managing the unmanaged devices, move them to the list in the left.
5. Click **Finish**.

You can also schedule downtimes for the devices incase you do not want it monitored for a specified interval

Device Snapshot

OpManager's Device Snapshot shows the device health and that of its resources at a glance.

To view the snapshot page of the device, click the device name link in the map, or type the name of the device in the **Device Search** box and hit **Go**. If there are many devices satisfying the specified criteria, a list of devices are displayed with their IP Address and category. Click the device whose snapshot you want to view.

The descriptions for various sections of Device Snapshot are as follows:

Device Details: Displays the system's details such as the IP address, operating system, time stamp of previous and next polls and a description on the system hardware details. System description is seen on the SNMP-enabled devices.

Device Notes: This tab shows additional device details. You can add additional fields to denote the device details. Click the ✎. The added fields are displayed in the snapshot page.

Tools: The following actions can be done by clicking the respective icon:

- Ping
- Trace Route
- Browse
- Open a Telnet session [Note: Telnet is not enabled in IE7 in Windows and Firefox in Linux. Click here to configure the steps to enable Telnet in IE7 and Firefox.]
- Open Remote desktop connection [Note: RDP is not enabled in IE7 in Windows. Click here to enable.]

Today's Availability: Displays the device availability of the current day in the form of a pie graph. Click or to view the availability report for the past 7 days or 30 days respectively.

Response Time: Shows the current response time of the device. Click or to view the response time details for the past 7 days or 30 days respectively. Click to configure response-time based threshold.

Packet Loss: Shows the packet loss percentage for the device on that day. By default, OpManager sends 1 ping packet during a poll. The ping counts, retries, timeout etc are configurable in the file /conf/Ping.properties.

CPU Utilization: Shows the current CPU load of the device. Clicking the graph shows the trend chart of CPU utilization

Memory Utilization: Displays the current memory utilization of the device.

Disk Utilization: Displays the current disk usage of the device in case of servers.

Monitors: This tab lists different monitors for the device. Select each monitor section to view the monitors. You can add more monitors from the available template, or even remove the unwanted monitors from the device.

Notification Profiles: This tab lists the notification profiles associated to the device. You can add more profiles from here.

Interfaces: Displays the list of interfaces in the selected device with their status and other details. Click the interface name link to view its availability and graphs on traffic and bandwidth utilization.

Custom Links: You can links to other applications, websites or other pages of OpManager and access them from the snapshot page. Click on the Add link to add a custom link.

Actions Menu: List of actions that can be performed on the device include:

- Configure IPMI
- Update Status
- Rediscover Now
- Show Alarms
- Suppress Alarms
- Monitoring
- Delete
- Manage/UnManage
- Event Log Rules

Device Info Menu: The device information that can viewed from this menu include:

- Asset Details- The Hard Disk and RAM details are shown here. More detailed information is shown when integrated with ServiceDesk Plus.
- Installed Software- A list of software installed on the server is shown here and this information is retrieved using SNMP.
- Active Processes- A list of processes up and running in the server is shown and is again retrieved from SNMP.

Reports: Provides the report of the following

- At a Glance Report
- Custom Report

- Top Clients
- Top Triggered Rules
- Top URLs
- Top Denied Requests
- Top Attacks
- Top Conversations
- Top Protocol Groups

Viewing Asset Details

If you have both, OpManager and ServiceDesk Plus running in your network, you can view a detailed asset information of a device, provided the device is discovered in both the applications, and the ServiceDesk settings are configured in OpManager.

To view the Asset Details, select the device and click **Device Info --> Asset Details**. This will show the detailed asset information from ServiceDesk Plus.

If ServiceDesk Plus is not integrated, then make sure SNMP is enabled. The device name, the hard disk size, and the RAM size is gathered for SNMP-enabled devices.

To update these details incase you upgrade your systems, follow the steps given below:

1. Select the device and click **Device Info --> Asset Details**.
2. Enter the values of **RAM size** and **Hark Disk**.
3. Click **Save** to apply the changes.

Viewing Installed Software

OpManager provides you the information on the software installed and currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. Under **Device Info**, click **Installed Software.**

Configuring Additional Device Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

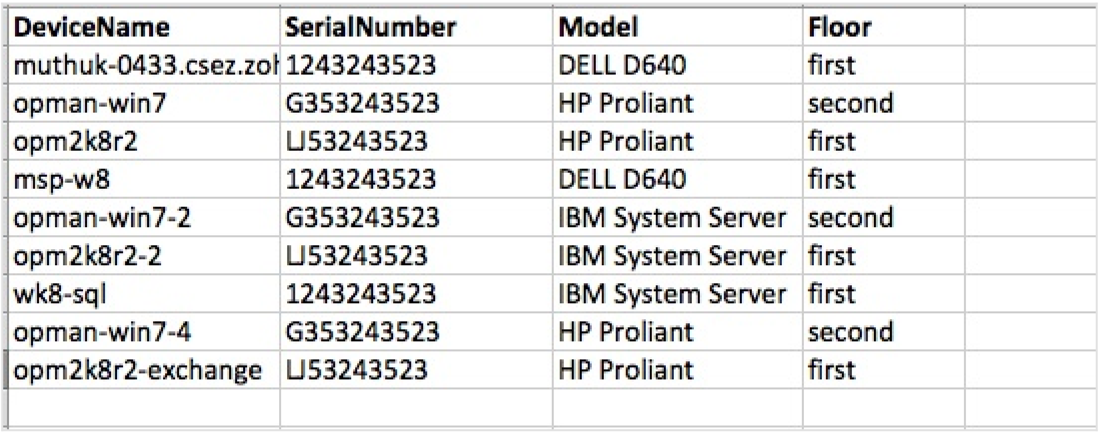
1. From **Admin** tab, select **Additional Fields**. A list of pre-populated fields is shown.
2. Select **Device** from **Associate pre-defined fields** to all list-box.
3. Click **Add Field** button on the top right corner of this table and configure the following values.
    1. **Field Name:** Configure the name of the additional
    2. **Type:** Select the property type
    3. **Field Length:** Set the length of the field.
    4. **Description :** Add a meaningful description for the field.
    5. Click **Save** to apply the configuration.

The properties added is applied to all the devices. The additional fields are displayed when you click the **Device Notes** tab in the device snapshot page. These properties are useful when configuring notification profiles. To delete these fields, select the corresponding check-box, and click the **Delete** link on the top right corner of this table.

Adding field properties in bulk

You can add field properties to multiple devices via a CSV file. Follow the steps given below:

1. Click on **Import Field properties from CSV** button.
2. Browse and select the CSV file. The CSV file should be in the following format



DeviceName	SerialNumber	Model	Floor	
muthuk-0433.csez.zoh	1243243523	DELL D640	first	
opman-win7	G353243523	HP Proliant	second	
opm2k8r2	LJ53243523	HP Proliant	first	
msp-w8	1243243523	DELL D640	first	
opman-win7-2	G353243523	IBM System Server	second	
opm2k8r2-2	LJ53243523	IBM System Server	first	
wk8-sql	1243243523	IBM System Server	first	
opman-win7-4	G353243523	HP Proliant	second	
opm2k8r2-exchange	LJ53243523	HP Proliant	first	

3. Click **OK**.
4. Map the **Field Name** with the **CSV Header**.
5. Click **OK**.

The field properties are applied to the devices successfully.

Configuring Additional Interface Properties

Configure additional properties of a device by adding additional fields. This makes device management easy.

1. From **Admin** tab, select **Additional Fields**. A list of pre-populated fields is shown.
2. Select **Interfaces** from **Associate pre-defined fields** to all list-box.
3. Click **Add Field** button on the top right corner of this table and configure the following values.
    1. **Field Name:** Configure the name of the additional property
    2. **Type:** Select the property type
    3. **Field Length:** Set the length of the field.
    4. **Description :** Add a meaningful description for the field.
    5. Click **Save** to apply the configuration.

These properties are useful when configuring notification profiles. To delete these fields, select the corresponding check-box, and click the **Delete** link on the top right corner of this table.

Configuring Device Dependencies

The status polling for a device can be controlled based on its dependency on some other device. This prevents the unnecessary status checks made to the dependent nodes.

For instance, many devices will be connected to a switch. If the switch goes down, all the devices connected to it will not be reachable. In this case, it is unnecessary to check the status of the dependent devices.

To configure the dependency for devices, follow the steps given below:

- In the **Admin** tab, under **Configuration**, click **Quick Configuration Wizard**.
- Select **Configure Device Dependencies** and click **Next**.
- Select the category of the device, Router, Switch, Firewall or Server on which the dependency is to be configured. The devices managed under the chosen directory is listed. Choose a device and click **Next**.

Configuring dependencies in individual devices

You can also configure dependencies for a single device from the device snapshot page. Here are the steps:

1. Go to the device snapshot page.
2. From the device details, click the link against the property **Dependency**.
3. Select the device on which it is dependent.

OpManager stops monitoring the devices if the dependent device is down. Configuring dependencies prevents false alarms.

Adding Custom Links to Devices

You might want to access another link either for reference or to another machine in your network over the web (like a VNC to another device for instance). You can add custom links from the snapshot page.

Here are the steps for creating custom links:

1. Go to the device snapshot page.
2. Click Custom Links > Add.
3. Provide a link name
4. Specify the Url that you intend accessing from this device.
5. Associate the link either to that device, or to all devices, or select devices, and save the configuration.

You will now be able to access the links from the snapshot page.

Administratively Disabling an Interface

If you want to administratively disable an interface, it is possible with OpManager in just a few clicks. Here are the steps:

1. Go to the required snapshot page of the interface that you want to disable.
2. Under Interface tab, click the **Disable** button.

The interface gets disabled and the interface's status is changed to Down. To enable the interface again, go to its snapshot page and click the **Enable** button under the Interface tab.

Classification and Device Templates

During initial discovery, OpManager categorizes the network devices into servers, printers, switches, routers and firewalls. For proper classification, install and start the SNMP agent on all the managed devices.

OpManager comes with over 600 device templates which carry the initial configurations to classify the devices into the pre-defined categories, and to associate monitors to them. The device templates enables you to effect a configuration once and is applied to several devices at a time whenever there is a change.

The templates carry the information required to classify the devices and to associate relevant monitors. You can define your own templates and modify the existing ones.

Creating/Modifying Device Templates

1. Go to Admin --> Device Templates
2. Click 'New Template' to define a template for a new device type. Click the Template name to modify an existing one.
3. Configure/Modify the following properties:
   - **Device Template**: Specify the device type.
   - **Vendor Name**: Select the vendor. Click **Add New** to add a new vendor, and **Save**.
   - **Category**: Select the category for the device type. On discovery, the devices are automatically placed in the select Category map.
   - **Monitoring Interval**: Configure the interval at which the device needs monitoring.
   - **Device Image**: Select the image for this device type.
   - **System OID**: Type the sysOID and click **Add**. Click **Query Device** for OpManager to query the device for the OID. You can also add custom OID in addition to the sysOID by clicking the edit icon. This will be helpful if you want to monitor customized Linux systems.
   - **Add Monitor**: Click this option to select the monitors.
   - **Edit Thresholds**: Click this option to edit thresholds.
   - Click **Create** button to create the new device template.

The classified devices are placed under different maps for easy management. For proper device classification, make sure you have installed and started SNMP in all the network devices before starting OpManager service.

The default maps include:

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- Printers
- Virtual Device
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

You can also add your own infrastructure views. Custom infrastructure views can be added to group devices which cannot be classified under the default views provided. For instance, if you would like to monitor some IP Phones, it will not be appropriate to classify them as servers or desktops.

This initial classification may not be accurate if

- the network devices do not support SNMP.
- some devices have their SNMP settings different from those specified in the Credential Settings.

Using Interface Templates

Monitoring requirement differs for different interfaces on a device. OpManager allows you to define configuration templates for interfaces of specific types. For instance, the configurations specified for an Ethernet interface can be applied to interfaces of this type across all devices, saving a lot of time.

1. Go to Admin a Interface Templates
2. Click an Interface Template to modify its properties.

The changes are applied to all interfaces of the same type.

Categorization into Default Maps

Devices are categorized into the following default maps in OpManager: The classification is done using SNMP and NMAP..

- Servers
- Routers
- Desktops
- Switches
- Firewalls
- DomainControllers
- Load Balancer
- WAN Accelerator
- Wireless
- UPS
- Printers
- Virtual Device
- Unknown
- Storage
- URLs
- WAN RTT Monitors
- VoIP Monitors

The discovered devices are classified into the above categories based on response to SNMP requests sent by OpManager to the devices. The devices that are not SNMP enabled, and the device types which are not included in the template are incorrectly classified under desktops. You can also add your own infrastructure maps to group your devices according to categories, or create business views to logically group devices, for instance, based on geography.

Adding New Infrastructure Views

You can create more defined groups under infrastructure views by adding more custom views. For instance, you might want to group all your Environment Sensors or IP Phones into separate infrastructure views. You can add a new infrastructure view from Maps tab or Custom dashboards.

Adding New Infrastructure View from Maps tab

Here are the steps to add a new infrastructure view from Maps tab:

1. From the pop-up in the Maps tab, click **Add Infrastructure View** option .
2. Specify the category **Name** and click **Add**.
3. From the listed devices, select and move the required devices to this view.
4. Click **Import Now** option.

The selected devices are displayed in the newly created infrastructure views.

Adding New Infrastructure View from Custom Dashboard

OpManager allows you to add a new infrastructure view from the dashboards also, provided if the infrastructure view widget is selected to get displayed in the dashboard. To add a new infrastructure view from the infrastructure widget, follow the steps given below:

1. Click **New Infrastructure View** link available at the bottom of the Infrastructure snapshot widget. Add category window opens.
2. Enter the **Category Name**.
3. Select the category whose properties needs to be inherited for this category.
4. Click **Add** button. Import window opens.
5. From the listed devices, select and move the required devices to this view.
6. Click **Import Now** button to start importing the selected into this category.

After you create new infrastructure views, you can create device templates for devices of this category. This allows you to define monitors specific to the category and automatically applies the configurations defined in the template to the devices as soon as they are discovered.

Sorting Devices in Maps

You can sort the devices on maps by the Name, Display Name, Device Type, or the Severity of the device. This helps you locate a resource faster.

To sort the devices in a map, from the **Sort By** combo-box, select the required option based on which you need the sorting to be done.
Note: Sorting of devices is supported only in the default maps.

Different Types of Map Views

Three different types of views are supported for the default maps. Click the **Select View** combo-box on the top right corner in the **Servers**, **Router**, and **Switches** maps to select the required view type:

1. **Details**: This is a list view of all devices on that map. This is useful when you have a large number of devices on a map.
2. **Large**: This shows bigger device icons, and gives more visibility. For instance, in the Servers map, the device icon also shows a couple of TCP Services monitored on the server indicating the service status. In the Routers and Switches map, all the interfaces are also shown in the map.
3. **Small**: This shows small device icons. The Router/Switch maps show only the parent devices, and in the Servers map, the services are not displayed.
4. **List View**: This list all the devices along with its status, IP Address, CPU & Memory utilized. From here you can apply device template, credentials, notification profiles etc. More.

Import Devices

A few devices are classified into Desktops map even if they are not desktops. This happens when either SNMP is not enabled on the device, or that particular device does not have a device template. You can import these devices into the correct maps as follows.

1. Go to the Map into which you want the devices imported.
2. Click the **Import** button on the top right corner. A corresponding dialog opens.
3. From the **Available Devices** list, select the devices and move them to the **Selected Devices** list.
4. Click **Import Now** to import the devices into the required category.

For instance, if a Router is classified into Desktops, go to the Router map and import the Router.

Adding a Domain

To add a domain:

1. Go to **Admin**-> **User Management**-> **Windows Domain**-> **Add Domain**.
2. Enter the **Domain Name**.
3. Enter the **Domain Controller** name.
4. Select **Enable Auto Login**.
    1. Select either **All Users** or **Selected Groups**.
       All Users: The auto login will be enabled to all the users. Select the permissions that you want assign - Read Only or Full Control.
       Selected Groups: The auto login will be enabled to the groups you specify. Enter the name of the groups in Read Only and Full Control columns. The access to groups will be enabled accordingly. Note: Configure one Group Name per line. The names are case-sensitive and should be configured as given in your AD.
5. Click **Add**.

A new domain has been successfully added.

Create New Users

You can create users in OpManager and provide required privileges to them. The option to create users is available only for the **admin** login account or those accounts which have 'Full Control' privilege.

Steps to add a user:

1. From **Admin** tab, click **User Manager**.
2. Click **Add Local User** option in the User Configuration screen.
3. Select any of the following user type

- Local user
- AD user
- AD group

Adding a Local user

1. **Login Details**:

   User Name - a user account name

   Password - a password for the above user

   Re-type Password- retype the password for confirmation
2. **Contact Details**:

   Email ID - email ID of the above user

   Phone number: the user's phone number

   Mobile number: the user's mobile number

   Twitter ID: Specify the Twitter user ID to enable tweeting of alerts.
3. **Access Details**:

   User Permission- Select the permission as **Full Control** to provide complete admin privilege to the user, or select **Read-only Access** to restrict the scope of the user to only read operations. A user with this permission can only view the details.

   Has access to - You can provide this user an access to either **All Devices,** or only specific **Business Views**,and/or **WAN**
4. Click **Add User** to add the user according to the scope specified here.

Logout and try logging in as the new user and check the privileges.

AD user

1. **Login Details**:

   User Name - Name of the AD user to be added.

   Select AD Domain - Select the desired AD domain from the list of available domains.
2. **Contact Details**:

   Email ID - email ID of the above user

   Phone number: the user's phone number

   Mobile number: the user's mobile number

   Twitter ID: Specify the Twitter user ID to enable tweeting of alerts.
3. **Access Details**:

   User Permission- Select the permission as **Full Control** to provide complete admin privilege to the user, or select **Read-only Access** to restrict the scope of the user to only read operations. A user with this permission can only view the details.

   Has access to - You can provide this user an access to either **All Devices,** or only specific **Business Views**, and/or **WAN**.
4. Click **Add User** to add the user according to the scope specified here.

Logout and try logging in as the new user and check the privileges.

AD group

1. **User Group Details:**

   Select AD Domain: Click on the drop down menu and select the desired AD domain from the list of available domains.

   Add Domain: Add a new domain that’s not present in drop down menu.

   Domain Controller: Update/provide the name of the AD domain controller. The domain controller name gets loaded automatically, once you select an existing AD domain.

   Enabling auto login: You can allow "All Users" (or) "Users from Selected Groups" under the chosen AD domain to access OpManager using their AD credentials. If you have chosen Selected Groups, provide the list of group names that require full or read-only access control. In case if the same user exist in both groups with read only and full control user permissions. The user with read only permission gets the preference over the other.
2. **Access Details:**

   User Permissions: Select "Full Control" to provide complete read/write control to the user to monitor resources using OpManager. Select "Read Only Access" if the user is allowed only to view the resources.
3. Click **Save**.

Changing User Passwords

You can change the password for the users. Either the **admin** user or an user with full control privilege only can change the passwords.

1. Go to Admin --> User Manager.
2. Click the Edit icon against the user name whose password you want changed.
    1. **Password Details**:
       Password - a password for the above user
       Re-type Password- retype the password for confirmation

    2. **Contact Details**:
       Email ID - email ID of the above user
       Phone number: the user's phone number
       Mobile number: the user's mobile number

    3. **Access Details**:
       For users with only partial permission, the business views assigned to that user is displayed. Remove selection for the view if you want to remove the views from the user's purview. For users with full control, this option is not displayed.

Removing Users

You can remover the users.

1. Go to Admin --> User Manager.
2. Click the Delete icon against the user name whose account you want to delete.
3. A confirmation dialog pops up. Click **OK**. The user account is deleted.

Monitoring CPU, Memory, Disk Using SNMP

The monitors for CPU, Memory, and Disk Utilization are automatically associated for the devices based on the device template definitions. For instance, for Linux servers, the default template has SNMP-based monitors associated. So, all Linux servers will have SNMP-based resource monitors associated. You will see the dial graphs for these three resources in the device snapshot page if SNMP is enabled.

All the Server templates have the monitors defined for various host resources. By default, the CPU, Memory, and Disk Monitors are associated to the servers. The device snapshot page shows the values of these monitored resources with dial-graphs.

If you do not see these monitors associated to the devices, it could be due to any or all of the following reasons:

- These monitors are not present in the device template.
- SNMP is not enabled on the device. In such case, enable SNMP and add the monitors to the device once again.
- Incorrect SNMP credentials are associated. Check the credential details like the SNMP version, community string etc.

Steps to add the monitors to the device again:

1. From the device snapshot page, select the Monitors tab.
2. From the monitor types, select Performance Monitors.
3. You will see the monitors displayed on the right if associated. Click Add Monitors link on the right.
4. From the list of monitors, select the SNMP monitors for CPU, Memory, and Disk Utilization.
5. You can also add other required monitors like Partition monitors etc.
6. The selected monitors are associated to the device and the resources are monitored.

To check if the SNMP agent in the device returns response, try the following:

1. Click the Edit icon against any of the associated monitor names.
2. From the edit screen, click **Test Monitor** link. This does a dynamic query to the device for the value of the selected resource, and show the data.

Incase the agent does not respond, you see a message to this effect. Refer to the troubleshooting tips to resolve the issue.

As an alternative, you can monitor the non-SNMP Linux servers using CLI (telnet or SSH), or the non-SNMP Windows devices using WMI.

Monitoring Resources Using WMI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP windows devices can be monitored using WMI. All the Windows device templates have the resource monitors preconfigured. All you will need to do is, disable the SNMP monitors associated and select the WMI monitors and associate them to the required devices.

Prerequisites

For monitoring the Windows environment, OpManager must necessarily be installed on a Windows machine. Besides, the device where OpManager is installed and the monitored remote Windows devices must have WMI, RPC, and DCOM services enabled on them. Authentication to the remote devices using WMI requires you to login as a domain user with administrator privileges. This is a requirement of the WMI protocol. If the device is in a workgroup, the system user name and password should suffice.

Steps to configure WMI Monitoring

Go to the device snapshot page.

1. From Monitors --> Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitors link on the right bottom.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as WMI against the monitor name.
4. Click OK. The monitors are added in the template under the Monitors column.
5. Click Apply. All the Windows devices to which the monitors are associated are listed. Another column also displays devices which are classified as 'Unknown'. You can pull the required devices from this list too. Click Apply once again.

The WMI-based monitors are associated to the device.

Monitoring Resources Using CLI

OpManager monitors the system resources using SNMP by default. However, in the absence of SNMP on the devices, the non-SNMP Linux devices can be monitored using CLI, ie., Telnet or SSH.. All the Unix Servers templates have the resource monitors preconfigured. All you will need to do is disable the SNMP monitors associated and select the CLI monitors and associate them to the required devices.

Prerequisites

For monitoring the unix servers, make sure either Telnet or SSH is enabled on them.

Steps to configure Telnet/SSH Monitoring

Go to the device snapshot page.

1. From Monitors --> Performance Monitors section, remove the SNMP-based monitors if any.
2. Click Add Monitors link on the right bottom.
3. Now, from the list of resource monitors, select the CPU, Memory, and Disk Utilization monitors which has the protocol name as CLI against the monitor name.
4. Click OK. The monitors are added in the template under the Monitors column.
5. Click Apply. All the servers to which the monitors are associated are listed. Another column also displays devices which are classified as 'Unknown'. You can pull the required devices from this list too. Click Apply once again.

The CLI-based monitors are associated to the device.

Adding More Monitors

Following are the monitors associated by default for the different device categories:

- **Servers**: CPU, Memory, Disk Utilization
- **Routers**: CPU, Memory, Buffer Hits/Misses, Temperature
- **Switches**: CPU, Memory, BackPlane Utilization
- **Firewalls**: CPU, Memory, and Connection Count.

Similarly, other categories also have few resources monitoring triggered by default. Besides the ones automatically associated, you can monitor more parameters. Here are the steps to configure more monitors:

1. From Admin, select Device Templates.
2. From the list of templates, select the template for the device type to which you want to associate more monitors. Select the corresponding letter to get to the template quickly.
3. In the device template, from the **Monitors** column, click the **Add Monitor** button.
4. All the predefined monitors are listed. Select the required monitors from here and click OK.
5. All the devices of the same type are listed. Click Apply for the selected monitors to be associated to all the selected devices.

Adding Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the SNMP-enabled devices in your network. The SNMP variable for which you intend configuring a monitor can return either a numeric or a string output when queried.

To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to **Admin** --> **Device Templates**.
2. Select the template in which you want to add a new monitor. Eg: Linux. Click the letter L to displays templates starting with this letter.
3. From here, click any template. Example - Linux. Scroll down the template and click **Add Monitors** under Monitors column.
4. Click the **New Monitor** link in this page.
5. Click the **Select** button in the Add a new monitor page to browse and select the OID for which you want add a monitor. The MibBrowser is shown.
6. Load the required MIB and select the OID. Eg: hrStorageSize from HostResource MIB. Click **OK** after selecting this OID.
7. Configure all the other properties of the monitor like the name, display name, units etc. Click **OK**. The new custom monitor is listed under Monitors column in the template.
8. Click **Apply**.
9. The devices are listed prompting you to select the devices for which you want the monitor to be associated. Check the list of devices and click **Apply**.
10. The modified template is applied to all devices of type Linux. Go to the snapshot page of any of the Linux devices. You will find the new custom monitor in the list of associated performance monitors.
11. For SNMP-based monitors to work, make sure to enable SNMP on the devices and check if the OID is implemented.
12. To easily apply a new monitor to a set of devices, you must add the monitor to the device template.

Consider the example given below to add a custom monitor that monitors a SNMP variable which returns a string output when queried.

1. Go to the **Linux template** page.
2. Click on **Add Monitor**s under Monitors column.
3. Click on **New Monitor** in the Add Monitors page,
4. Click on **Select** button in order to open the MIB browser.
   1. Select **RFC 1213** MIB and click on **Expand All** .
   2. Choose the **System Name** variable. The OID of it will be displayed at the bottom. [This variable will give the System Name of the device when queried].
   3. Click on **OK**. The OID will be displayed in the SNMP OID field.
5. Configure all the other properties of the monitor like the name, display name, units etc. Click **OK**. The new custom monitor is listed under Monitors column in the template.
6. Click on **Apply** to add the template to the devices.
7. The devices are listed prompting you to select the devices for which you want the monitor to be associated. Check the list of devices and click **Apply**. The monitor will be associated to the selected devices under performance monitors.

Adding WMI-based Custom Monitors

In addition to OpManager's default monitors, you can also create your own monitors for the WMI-enabled devices in your network. To add a custom monitor for a resource of a particular device type, the device template must be modified. The new monitor should be defined in the device template so that the monitor is associated for all devices of that type. Here are the steps.

1. Go to **Admin** --> **Device Templates**.
2. Select the template in which you want to add a new monitor. Eg: Windows XP (Click the letter W to display templates starting with this letter).
3. From here, click any template. Example -Windows XP. Scroll down the template and click **Add Monitors** under Monitors column.
4. Click the **New Monitor --> WMI** link in this page.
5. Select a device name that OpManager can query. OpManager executes a WMI query on the device and checks the response.
6. Specify the WMI credential to be used for that device. OpManager needs to authenticate itself to the device using the WMI credential specified.
7. Configure the interval at which the resource should be monitored and click Next.
8. Select the WMI Class to list the performance counters present in that WMI Class.
9. Select the Performance counters and the instances (the instances are also listed here) that require monitoring and click on **OK**. The monitors are added to the template.
10. Click on **Apply** to apply this template to the required Windows devices.

Applying the template to the other devices, adds the new custom monitors to all the selected devices, and the selected resources are monitored at the interval configured in the template.
Note: While selecting the WMI class, current value shown on mouse over is the raw data and it is NOT the value calculated using the appropriate counter type of the WMI performance counter.Upon associating to devices, counter values will be calculated based upon the counter types.

Device-specific Monitors

The monitoring configuration may need alteration for specific devices. Doing a bulk-configuration using the device templates, applies the same set of configurations for the devices of the same type. In order to change the configuration for specific devices, here are the steps:

1. Go to the device snapshot page.
2. Scroll down to the Monitors section.
3. From here select the required monitors. Monitors of the selected category are listed on the right.
4. Click the Edit icon against the monitor name. The Edit Monitor page is displayed.
5. Change the values for the required parameters and and click OK.

The changes to the monitor are effected only for that device.

Configuring thresholds for monitors

Configuring thresholds enable OpManager to proactively monitor the resources and the services running on the servers and network devices, and raise alerts before they go down or reach the critical condition. OpManager offers multiple threshold levels namely Warning, Trouble and Error for breaking the fault into three stages and taking corrective actions accordingly.

- Warning threshold - low severity
- Trouble threshold - medium severity
- Error threshold - high severity

You can configure multiple thresholds for the monitors that are associated to a single device, configure from the device template in order to apply across multiple devices and also configure from Quick Configuration Wizard.

Configure threshold limits for the monitors associated to a single device

1. Go to the device snapshot page.
2. Under Monitors tab, click on the edit icon corresponding to the monitor for which you want to configure threshold limits. Edit Monitor page opens.
3. Ensure that the **SNMP OID** and the monitoring **Interval** are configured.
4. Specify the unit for the monitored resource in terms of percentage, MB, KB etc (based on how the parameter is measured).
5. Select the condition [>,=, <, or !=] for Warning Threshold, Trouble Threshold & Error Threshold, and enter the value. Alert is raised if the monitored value is greater than, equal to, not equal to, or lesser than (which ever is selected) the threshold value.
6. Enter the **Rearm Value**. Rearm value is the value which the determines the monitor has restored to normal condition. For instance, the Warning threshold condition for a memory monitor is selected as greater than [>] and the threshold value is configured as 75. The monitored memory value of that device is 80. Now alert is raised and the monitor is in violated condition. At the next poll the monitored value is 72. An alert for returning to normal condition is generated. At the next poll again the monitored value goes to 80. Again a threshold violation alert is generated. In order to avoid this, enter the rearm value. Only if the monitored value reaches the rearm value the monitor goes to the normal condition and a normal alert is raised. Note: If you select the threshold conditions greater, then the rearm value should be lesser than the threshold value and vice versa.
7. In the **Consecutive Times** field enter the value of how many consecutive times the thresholds (Warning, Trouble and Error) can be violated to generate the alert.
8. Click on **Advanced** button to configure the Alarm Message and Severity. Based on the monitor, the values for Alarm message and severity are pre-configured by default.
9. Click on **OK**.

Configure threshold limits for the devices from their device template page

1. Go to the Device template page.
2. Under **Monitors** tab, all the monitors that are currently associated with the devices are listed. If you want add or remove required monitors. Click on **Edit Threshold** button. Edit Thresholds page opens.
3. Configure the Warning Threshold, Trouble Threshold, Error Threshold and Rearm Value and click on **OK**.
4. Click on **Apply**.
5. Select the devices for which you want to associate the monitors from the left column and move to the right column.
6. Again click on **Apply**.

Configure thresholds for multiple devices from Quick Configuration Wizard

1. From **Admin** page, click on **Quick Configuration Wizard**.
2. Select **Add Performance monitors to several devices (SNMP, WMI and CLI)** option and click on **Next**.
3. Open the required device template page and follow the steps from 2 to 6 of Configure thresholds for the devices from their device template page.

Viewing Process Diagnostics

You can view the top ten processes utilizing the maximum resources. Process statistics is retrieved using Telnet/SSH/WMI, for which the correct credential must be associated to the devices. To be able to view the diagnostics,

1. Configure relevant CLI and WMI credentials.
2. Click the 🔍 link on top of the dial graphs for CPU, Memory, and Disk graphs. The top 10 processes are shown.

You can also end the processes from here.

Viewing Live Workload on CPU, Memory and Hard disk

OpManager provides you the option to view the workload handled by the CPU, Memory and Hard disk of a device in real time. This option is very useful in cases where you would have restored a device just a short time back and want to continuously monitor for few minutes. To view the live workload,

1. Go to the device snapshot page.
2. Click on the Real Time icon available on top of the CPU, Memory and Hard disk dials to view the live workload.

The amount of CPU/Memory/Hard disk that is being currently utilized by the device is displayed in a graph in terms of percentage for the configured Refresh Interval and Time Window.

Viewing Live Interface Traffic

OpManager provides you the option to view the traffic handled by an interface in real time. Here are the steps:

1. Go to the device snapshot page.
2. Click on **Interfaces** tab. All the interfaces of the device gets listed.
3. Click on the respective Real Time icon of the interface whose live traffic has to be viewed.

Live In and Out traffic in the interface is displayed as a graph for the configured Refresh Interval and Time Window.

Viewing Live Temperature

OpManager provides you the option to view the temperature of the router in real time. Here are the steps:

1. Go to the snapshot page of the router.
2. Click on the Real Time icon available on the temperature value that is displayed.

Live temperature of the router is displayed as a graph for the configured Refresh Interval and Time Window.

Modifying Live View Parameters

Live View displays the resources utilized, temperature and traffic details as a graph for the configured Refresh Interval and Time Window. Refresh Interval determines the interval between successive polls to the resource and the Time Window determines the period for which the data has to be displayed continuously. By default the Refresh Interval is 1 second and the Time Window is 5 minutes. To modify the default Refresh Interval and Time Window values, follow the steps given below:

1. In the Live view window, click the **Configure** button.
2. Enter the required value in the **Refresh Interval** and **Time Window** fields.
3. Click **Modify** to effect the changes.

Monitoring Packet Loss for Devices

You can monitor the packet loss percentage on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the **Today's Packet Loss** value shown on the right.
3. Click the corresponding small icons to see the packet loss report for the last 7 or 30 days.
4. Click the icon to configure threshold value in percentage. If the packet loss percentage exceeds the threshold value, a threshold violation alarm is triggered. This alarm can inturn be notified.

Monitoring Response Time of Devices

You can monitor the response time on a per device basis and view even the packet loss reports.

1. Go to the device snapshot page.
2. Look at the **Response Time** value shown on the right to know the device response time..
3. Click the corresponding small icons to see the response time report for the last 7 or 30 days.
4. Click the icon to configure threshold value in milliseconds. If the device response time exceeds the threshold value, a threshold violation alarm is triggered. This alarm can inturn be notified.

Monitoring TCP Services

OpManager provides out-of-the-box support for the following services: Web, HTTPS, FTP, IMAP, LDAP, Telnet , MySQL, MS-Exchange, SMTP, POP3, WebLogic, Finger, Echo, DNS, and NTTP. By default, during discovery, OpManager scans the devices for the services: DNS, MSSQL, MySQL, Oracle, SMTP, Web. You can also select other services in the list. When they are found running on their default ports, OpManager starts monitoring the services.

Scanning Services during Discovery

By default, OpManager scans each device on the network for the services that are chosen during discovery.

To modify this list, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Discovery**, click **Services**.
3. Select the check boxes under **Scan during discovery?**, corresponding to the services to be discovered and clear the selection for the services that are not to be discovered.
4. You can modify the service monitor properties in OpManager. When the service is not running on the default port, you can configure the actual port in which it is running, and you can change the timeout interval. **Save** the changes.
5. Click **Update** to apply the changes.

OpManager allows you to change the settings for monitoring these services as per your network needs. You can configure new services that are not available in the list. OpManager can manage services running on standard TCP ports.

Note:

- The list contains the service names and the corresponding port numbers. To edit the settings of any of the available services, click Edit icon.
- If you do not find the service you want to manage in the list, you can add the service by clicking **Add Service** under **Actions** menu. For details, refer to Adding a New Service.

Viewing Service Status and Response Time

1. Go to the device snapshot page.
2. Under **Service Monitors**, you will see the list of services managed in the device, if any, with their status and current response time.
   - Click the service name to view the historical report on the response time and the availability chart of the service.
   - Click the Availability chart to view the service downtime/uptime chart, summary and historical information.

Configuring Alerts

By default OpManager raises an alarm if a service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page.
2. Under **Service Monitors**, click on the service name to open the service snapshot page.
3. Modify the count entered for '**Generate alarm if unavailable for _ consecutive times**' by clicking the edit icon. For example if you enter the value as 2, OpManager will raise alarm only if the service is unavailable for 2 consecutive polls.
4. Update the value and click the save icon.

Monitoring TCP Services on a Device

To select the services to be monitored in a device, follow the steps given below:

1. Click the Server in the map.
2. In the Monitors section, select **Service Monitors** to see the monitors listed.
3. Click **Add Monitor** at the bottom of this list to see the complete services list..
4. Select the services to be discovered from the list and click **OK**.

Adding New TCP Service Monitors

You can add new TCP services for monitoring.

1. Go to Admin --> Services Monitors
2. From the Actions menu in this screen, select **Add Service**.
3. Specify the name of the TCP service that you want to monitor.
4. Specify the TCP Port number that has to be checked for service availability
5. Specify the timeout interval in seconds for the port-check request.

Associating the Service to Devices

To associate a service to a server,

1. Go to Admin --> Service Monitors
2. From the Actions menu, select **Associate**.
3. Select the required TCP service from the list of services displayed.
4. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
5. Click Save.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Add a new service monitor to several devices** and click Next.
3. Now, select **Associate a service to servers** option and click Next again.
4. All the available TCP services are listed. Select the service which you want to monitor on your servers. Click Next.
5. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
6. Click Finish. The service monitor is associated to the selected devices.

Monitoring Windows Services

Certain applications in Windows machine run in the background as services. OpManager discovers and monitors the status of such services using WMI. OpManager generates alarms whenever they fail.

Prerequisites

To monitor Windows services, OpManager should be installed in a Windows machine. OpManager uses WMI to monitor the Windows services and hence you need to provide the log on details of a user with administrative privilege to connect to the device. So, make sure you configure a WMI credential so that you can apply this to the windows devices.

Associate Windows Services to a Device

To monitor a Windows service, follow the steps given below:

1. Go to the device snapshot page.
2. Confirm if the correct WMI credential is associated to the device. Else, configure the password details in the device.
3. Click **Add Monitor** in the **Windows Service Monitors** section. This option will be available only for Windows servers.
4. Select the services to be monitored in the device and click **OK**.

Associate Windows Service Monitors to several devices

1. From the Admin tab, select Windows Service Monitors.
2. Select **Associate** option from the Actions menu.
3. From the drop-down list box, select the services one-by-one and move the devices from the 'not monitored' column to the 'monitored' column.
4. Click Save.

The selected service monitor is added to the device.

Using Quick Configuration Wizard

You can also use the Quick Configuration Wizard to associate a service to several devices at one go. Here are the steps:

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Add a new service monitor to several devices** and click Next.
3. Now, select **Associate a Windows service** option and click Next again.
4. All the available Windows services are listed. Select the service which you want to monitor on your servers. Click Next.
5. Select the devices on which you want to monitor the service from the column on the left and move them to the right.
6. Click Finish. The service monitor is associated to the selected devices.

Configuring Alerts

By default OpManager raises an alarm if a Windows service is down. If required you can configure OpManager to raise an alarm if the service unavailable for a N number of times consecutively.

1. Go to the device snapshot page.
2. Under **Windows Service Monitors**, click on the edit icon corresponding to the Windows service for which you want to configure the alert.
3. Modify the count entered for '**Generate alarm if unavailable for _ consecutive times**' by clicking the edit icon. For example if you enter the value as 2, OpManager will raise alarm only if the service is unavailable for 2 consecutive polls.
4. You also have to option to either restart the service or restart the server if the service goes down. Select the check box and appropriate radio button.
5. Click the **Save** button.

Adding New Windows Service Monitors

In addition to the Windows services monitor supported by OpManager out-of-the-box, you can add monitors for other windows services too..

To add a new Windows service monitor, follow the steps given below:

1. Under the **Admin** tab, click **Windows Service Monitors**.
2. Under **Actions**, click **Add Service**.
3. Type the name of the device in the **Device Name** field.
4. Type the domain administrator user name password for the device in the respective fields and click **Next**.
5. A list of all the Windows Services available on that machine is displayed. From this select the services that you want monitored across all other Windows Servers.
6. Based on whether or not you want to restart the service or the machine when the service goes down, select the corresponding option.
7. Click **Finish**. A list of Services for which a monitor is added is shown.
8. Click the link at the bottom of this list to associate these service monitors to devices.
9. From the drop-down list box, select the services one-by-one and move the devices from the 'not monitored' column to the 'monitored' column.
10. Hit **Save**.

The newly added services are also monitored on the selected servers.

Monitoring Processes on Windows/Unix Servers & Desktops

OpManager provides out-of-the-box support for monitoring the availability of all the processes running on a Windows or Unix system. Windows systems uses WMI and Unix systems uses CLI to monitor the processes that are running on the system.

Here are the steps for configuring Process Monitors:

1. Go to the device snapshot page.
2. Make sure you have associated the WMI/CLI Credentials to the device.
3. From the Monitors tab, click on **Process Monitors**.
4. Click on the relevant link on Process Monitors column on the right and select the required processes to be monitored.
5. Click OK to associate the monitors to the device.

Configure Thresholds for Process Monitors

You can set resource thresholds for the Process Monitors. Once a resource (cpu/memory) utilization by a process exceeds the configured threshold, an alert is triggered.

1. Click the Edit icon against the process name.
2. Configure the threshold values for CPU and Memory resources.
3. Configure the number of times you would like to allow threshold violation before being notified. For instance, if you configure the value as 3, OpManager notifies you if the resource threshold is violated 3 consecutive times.
4. Configure the number of the process instances, exceeding which you would like to be notified. For instance, if you would like to be notified if the number of Apache.exe instances on the monitored device exceeds 3, configure the value here as 3 and save the changes.

Alerts are fired based on the above settings.

You can also view active processes on a device and also view the process diagnostics against a system resource.

Viewing Active Processes

OpManager provides you the information on the processes that are currently running on the managed device. You need to have SNMP agent running in the device to view this information.

To view the details, click the device icon in the map. From the snapshot page, under **Device Info** menu, click **Active Processes**.

Adding New Process Template

Process templates helps you to select the processes that are running on a device, convert each of them into individual templates and apply all of them across multiple devices. To add a new process template,

1. Go to **Admin**-> **Process Templates**.
2. Click **Add New**. Add New Template window opens.
3. **Device Name**: Select the device which runs the process(es) that needs to be converted into template(s).
4. **Protocol**: Select the relevant protocol to access the device.
5. Configure the correct credentials. Note: If new credential settings have to be configured, then click **New** button.
6. Click **Next**. All the processes that are currently running on the device are listed along with their ID, Path and Arguments.
7. Select the required process(es).
8. Click **Add**. Associate process Template Window opens.
9. From the listed devices, select and move the required devices.
10. Click **Associate**.

The selected processes are converted into templates and associated across multiple devices.

Associating Process Template to Multiple Devices

To associate a process template across multiple devices, follow the steps given below:

1. Go to **Admin**-> **Process Templates**.
2. Click **Associate**.
3. Select the process template to be associated to multiple devices,
4. From the listed devices, select and move the required devices.
5. Click **Associate**.

The selected process template is applied across multiple devices.

Creating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters .

Follow the steps given below to add script templates

Enter the **command** to run the script, as if provided in command prompt.

Example:cscript ${FileName}.vbs
Note that ${FileName} must be followed by script file extension. You may also pass arguments. Argument list may use variable **${DeviceName}** which will be replaced with the monitored machine name in run time. Other supported variables are **${UserName}** - WMI/CLI username, **${Password}** - WMI/CLI password, **${SNMPRead}** - SNMP read community string. For example,cscript ${FileName}.vbs ${DeviceName} ${UserName} ${Password}Script Output FormatIn order to store the result of the script in DB, the output must be in the format given below.

```
Message:This message will be used as alarm message.
Data:
Instance1          value1
Instance2          value2
...                ...
InstanceN          valueN
```

Exit code will be used to set the status of the script monitor. Exit code "0" for up , any other exit code for down. Only numeric values are allowed as statistical data. The instance name and value must be separated by a TAB space(t). Status checking scripts may NOT contain data part. If there is no message in output, a default message will be used for alarm message.

Admin-> **Script Templates** (under Monitoring)-> **New Template**. 1.

name and **description** for the template. 2.

Monitoring Interval. 3.

Unit for the monitored parameter. 4.

5.

6.

7.

${TempDir} or 8.
${UserHomeDir} which means OpManager temporary directory and user's system home directory repectively.

Test Script to test the script. 9.

1. If required you can set threshold values:
2. Configure the threshold value and select the match condition.
3. Configure the **Rearm Value**.
4. Specify the number of times the threshold can be violated consecutively to raise an alarm.
5. Configure **Alarm Message** and **Severity**.

To disable threshold, click **Disable Threshold** link.

Save button to save the template. 10.

11.

Associate button. 12.

You have successfully created a script monitoring template and associated it to devices.

Editing Script Templates

To Edit a script template

1. Click on **Edit** icon corresponding to the script template that you want to edit.
2. Carry out the necessary modifications and **Save** it.

Importing/Exporting Script Templates

The import/export options allows you to share scripts that are created by you with OpManager community and use the scripts shared by others. Use this form to share the script with OpManager community.

Import scripts

1. Click on **Import** button that is available in the Script Templates page.
2. Click on **Browse** button to locate the script (.xml file).
3. Click **Import**.

The script has been successfully imported to OpManager.

Export Scripts

1. Click on **Export XML** icon corresponding to the script that you want to export.
2. Click on **Save** to save the script.

Copying Scripts

OpManager allows you to save a copy of the script, modify it and use it for other monitoring requirements.

1. Click on **Copy As** icon that is available in the Script Templates page. The script template opens.
2. Carry out the necessary modifications and **Save** it.

Deleting Scripts

To delete a script, click on the the **Delete** icon corresponding the script template.

Associating Script Monitoring Templates

Script Monitoring templates help you create custom scripts to monitor custom parameters .

Follow the steps given below to add script templates

1. Go to **Admin**-> **Script Templates** (under Monitoring)-> **New Template**.
2. Provide a **name** and **description** for the template.
3. Configure the **Monitoring Interval**.
4. Specify the **Unit** for the monitored parameter.
5. Enter the **command** to run the script, as if provided in command prompt.
6. Enter complete content of script file.
7. Enter the time to wait for script execution completion.
8. Select the machine from which you want to execute the script.
9. Provide the details of the directory from which you want to execute the script.
10. Click on **Test Script** to test the script.
    1. If required you can set threshold values:
    2. Configure the threshold value and select the match condition.
    3. Configure the **Rearm Value**.
    4. Specify the number of times the threshold can be violated consecutively to raise an alarm.
    5. Configure **Alarm Message** and **Severity**.

       To disable threshold, click **Disable Threshold** link.
11. Click on **Save** button to save the template.
12. Select the devices you want to which you want to associate this template, and move them to Selected devices column.
13. Click on **Associate** button.

You have successfully created a script monitoring template and associated it to devices.

Log File Monitoring

Every application prints status messages, error messages, and other critical information in its log. It is very tedious to skim through all these bulky log files for understanding the application performance. To manage such mission critical applications in real time, monitoring their log files is necessary. OpManager offers agent-based log file monitoring for real-time fault and performance management.

How log file monitoring works?

The log file monitoring agent installed in the end machine, monitors the log files continuously for the required string (It may even be a regex). Once that string is printed, it immediately notifies OpManager server, which in-turn raises the alarm.

Steps to add a log file monitor

Prerequisite: Before installing the agent, add that device in OpManager.

1. Install the agent in the end machine which has the log files.
2. Go to Admin-> File Monitoring Templates-> New Template.
3. Enter a template name, and path of the file.
4. Click Next.
5. Under File Contains row, enter the String to be searched. OpManager supports regular expressions as well. Note: All the special characters should be preceded by a backslash.
6. Select Match Case check box, if you want the search to be case sensitive.
7. Enter the number for consecutive times of the log print for which you want to raise the alarm.
8. Click Next and associate it to the required devices. You have successfully added a log file monitoring template.
9. Now map the agent to the device that you have added in OpManager (prerequisite).
    1. Go to Admin-> Agents. You can find the agent installed device listed.
    2. Select the respective device in the Mapped Device column.
    3. Click confirm to map the device.

You have successfully created a log file monitor.

Adding File Monitoring Template

You can now track changes on critical system and user files and be notified if a specific change occurs. For instance, you might want to be notified if the file size increases beyond a defined limit, if some files are missing, log prints etc. Configure meaningful templates in OpManager and apply them to devices on which you want the files monitored. Using the following file monitoring features you can monitor the following parameters:

File Content: Presence of a word/string or in a log file, supports regex as well
File size: Watch for an increase or decrease in the file size
Presence of a file: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
File age: Keep track of the age of a file and take actions based on the age
File modification: Be notified if a file has been modified

Steps to configure a file monitoring template

1. Go to **Admin**-> **File Monitoring Templates**.
2. Click **New Template**. Add New Template window opens.
3. **Template Name**: Configure a name for the template.
4. **File Path**: Specify the path in which OpManager should locate the file.
5. Polling Interval: Configure the interval at which OpManager should monitor the file.
6. Description: Provide a brief, meaningful description for the template and click Next.

Configuring Alerts for File Monitors

Configure the monitoring criteria based on which you want to be notified:

1. **File Contains:** To monitor the print of a word/string in a log file, you have to install log file monitoring agent in the end server where the application is running. Click on Agent link to download and install the agent. Once you install the agent, it looks for the specified string in the said log file. If the word/string is printed in the log file, OpManager raises alert. If required, you can configure the agent to match the case when searching for the word/string. The notification can be triggered if the alert condition is met the specified number of times.

2. **File Existence:** OpManager looks for the file in the specified path and alerts based on the conditions specified. You can configure to be notified if the file does not exist in the path specified, or be notified if the file exists , or you can choose not to monitor. Also, choose the severity that you would like to assign to this alert. The notification can be triggered if the alert condition is met the specified number of times. That is, OpManager alerts you if a particular file does not exist in a path during two consequetive polls.

3. **File Size:** Configure OpManager to alert you if the file size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Choose the severity that you would like to assign to this alert. The alert can be triggered if the threshold is violated a specified number of times.

4. **File Age:** Similarly, you can configure OpManager to alert you based on the age of the file. For instance, you can be notified if a file is over 20 days old.

5. **File Modification:** When a file is modified, the date on which the file is modified is updated. You can configure OpManager to notify you whenever there is a change in the date modified. This option helps you keep track of any changes done in critical files. Choose the severity that you would like to assign to this alert.

Associating the File monitor to devices

Having creating a template with the alert criteria, you can now associate the template to the devices.

1. After configuring the threshold details, click Next. The devices are listed on the left.
2. Select the devices for which you want to apply this template and move them to the right.
3. Click on Associate button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.

Prerequisite:

- Ensure that device in which in you are installing the agent has already been added in OpManager.
- Click on the download link to download the agent.
- Install it on the machine which has the log file. Double-click the exe to begin the installation.

Adding Folder Monitoring Template

Besides monitoring files on the systems, you can also monitor the folders.You can track changes in folders based on the folder size, the number of files in a folder etc. Again, like file monitors, you can be notified if a specific change occurs. For instance, you might want to be notified if the folder size increases beyond a defined limit, if some files in a folder are missing etc. Configure meaningful templates in OpManager and apply them to devices on which you want the folders monitored. Monitor the following parameters on folders:

- Folder size: Watch for an increase or decrease in the file size
- Existence of a file: Check the availability of a file in the specified directory (may have been moved, renamed, or deleted)
- Folder Modification: Keep track of changes (add/remove/rename) on the files or sub-folders with in a folder. However, sub-folder level changes are not monitored.
- File Name: Watch files in a folder by their name.
- File Size/Age: Check the last modified file or all files in a folder for file size and age.
- File count: Keep track of the number of files within a folder.

Steps to configure a file monitoring template

1. Go to **Admin**-> **Folder Monitoring Templates**.
2. Click **New Template**. Add New Template window opens.
3. **Template Name**: Configure a name for the template.
4. **Folder Path**: Specify the path in which OpManager should locate the file. You can either provide the local directory (C:) or UNC share path (\servernameSharedDirectory).
5. **Polling Interval**: Configure the interval at which OpManager should monitor the file.
6. **Description**: Provide a brief, meaningful description for the template and click **Next**.

Configuring Thresholds for Folder Monitors

Configure the monitoring criteria for Folder/File monitoring conditions based on which you want to be notified:

1. **Folder Existence:** OpManager looks for the folder in the specified path and alerts based on the conditions specified. You can configure to be notified if the folder does not exist in the path specified, or be notified if the folder exists , or you can choose not to monitor.
2. **Folder Size:** Configure OpManager to alert you if the folder size goes over, or comes below a specified size. Select the relevant threshold for alerting. You can configure the size in terms of bytes, KB, MB, or GB. Configure the rearm accordingly to reset the alarm.
3. **Folder Modification:** Select Alert if modified check box to receive alerts when files/sub-folders are added/deleted/renamed in the specified folder.
4. **File Filter:** By default all the files in the specified folder are monitored. Deselect All files check box and enter the file name or extension (*.pdf,*.txt) of the files alone you want to monitor. You can enter multiple values separated by comma, but no blank space is allowed. You can enter the filename in the following formats:
   - Full file name with extension ‘stdout.doc,stdlog.txt’
   - File name with wild characters ‘*out’ or ‘std*’. Files containing the same prefix or suffix name with same/different extension will be monitored
   - File name in date format ‘2011062200001.txt’. Enter the file name in a static format $YYYY$MM$DD*.txt or $YYYY $DD$MM*.txt
5. **File Name Contains:** OpManager looks for the files in the specified folder and alerts based on the conditions specified. You can configure to be notified if the folder does not contain any file in the specified name , or be notified if the folder contains

files in the specified name, or you can choose not to monitor.

6. **File Size/Age:** OpManager looks either last modified file or all files for file size and age. If the threshold condition for either file size or file age is violated, an alarm is raised. Configure the relevant threshold and ream conditions.
7. **File Count:** You can monitor the number of files specified in the File Filter and be alerted if the count changes, or of it violates a count threshold. Configure the rearm accordingly to reset the alarm.

Configuring Alerts for Folder Monitors

Configure the following alerting options:

1. **Severity:** Choose the severity that you would like to assign to this alert.
2. **Consecutive Times:** Specify how many time the threshold can be violated to generate the alert
3. **Alarm Message Format:** Configure the alarm message. You can include the alarm variables by appending $ to the variable name.

Associating the Folder monitor to devices
Having creating a template with the alert criteria, you can now associate the template to the devices.

1. After configuring the threshold details, click Next. The devices are listed on the left.
2. Select the devices for which you want to apply this template and move them to the right.
3. Click on Associate button at the bottom of the column to associate the template to all the selected devices.

The monitor is added to the device and OpManager alerts based on the alert conditions configured.

Active Directory Monitoring

Active directory monitoring feature takes OpManager a step further in proactive monitoring of Windows environment. The system resources of the Domain Controllers where the Active Directory (AD) database resides, and few critical Active Directory Services are monitored in OpManager.

To make AD monitoring more simple and easily accessible, The Domain Controllers are classified under a separate category under Infrastructure Views. The categorization of the device as a Domain Controller is done automatically if SNMP is enabled. The system resources of the device and the AD services are monitored using WMI.

The snapshot page of the Domain Controller shows a dial graph for AD Store in addition to the dial graphs for CPU, Memory, and Disk Utilization.

The other utilization data displayed in the snapshot page for the Domain Controller are:

- Resource Utilization by LSASS (Local Security Authority Subsystem Service)
- Resource Utilization by NTFRS (NT File Replication Service)
- Ad Store Utilization
- Performance Counters showing information such as the AD Reads, the AD Replication objects etc

Besides these, following are the AD Services monitors associated by default:

- **Windows Time service** : The service synchronizes the time between domain controllers, which prevents time skews from occurring.
- **DNS Client Service** : This service resolves and caches (Domain Name Server) DNS names.
- **File Replication Service** : This service maintains file synchronization of file directory contents among multiple servers.
- **Intersite Messaging Service** : This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport.
- **Kerberos Key Distribution Center Service** : This service enables users to log on to the network using the Kerberos version 5 authentication protocol.
- **Security Accounts Manager Service** : This service signals other services that the Security Accounts Manager subsystem is ready to accept requests.
- **Server Service** : This service enables the computer to connect to other computers on the network based on the SMB protocol.
- **Workstation Service** : This service provides network connections and communications.
- **Remote Procedure Call (RPC) Service** : This service provides the name services for RPC clients.
- **Net Logon Service** : This service supports pass-through authentication of account logon events for computers in a domain.

You can add more AD Monitors to be monitored by clicking the Add Monitor button.

Exchange Server Monitoring

You can monitor critical MSExchange (2000/2003/2010) Services and parameters using OpManager. Monitoring is done using WMI. Thresholds are pre-configured for critical services. You can also modify or enable thresholds for other services and parameters.

The services monitored are:

- Information Store
- Site Replication Store
- MTA Stacks
- Exchange Management
- SMTP
- POP3
- IMAP4
- System Attendant
- Routing Engine
- Event Service

The Exchange parameters that are monitored can be classified under the following categories:

- Address List Monitors
- POP3 and IMAP Monitors
- Information Store Public Folder Monitors
- Event Service Monitors
- SMTP Monitors
- Information Store Mailbox Monitors
- Message Transfer Agent Monitors
- Directory Service Monitors
- Information Store Monitors

Configuring Exchange Parameters and Services Monitoring

1. Go to the snapshot page of a device that has Exchange running.
2. Scroll down and select the **Monitors** tab.
3. Click on **Performance Monitors**. The monitors are listed on the right.
4. Click the **Add Monitor** button on the right. A list of monitors is displayed.
5. Click the **Exchange Monitors** button on top of this list. The monitors of all the Exchange parameters and services are displayed.
6. From this list, select the required Monitors and associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring MSSQL Parameters

MSSQL Services and Parameters can be monitored using WMI. Here are the steps to associate the MSSQL monitors to a device:

1. Go to the snapshot page of a device that has MSSQL running.
2. Scroll down and select the **Monitors** tab.
3. Click on **Performance Monitors**. The monitors are listed on the right.
4. Click the **Add Monitor** button on the right. A list of monitors is displayed.
5. Click the **MSSQL Monitors** button on top of this list. The monitors of all the MSSQL parameters are displayed.
6. From this list, select the required MSSQL Monitors and associate it to the Server.

These monitors are associated to the device. Ensure to associate the correct WMI credential to the device. OpManager uses these credentials to connect to the device using WMI.

Monitoring Windows Event Logs

The Event Log is a Windows service that logs about program, security, and system events occurring in Windows devices. The events can be related to some application, system or security. You can monitor these events using OpManager and configure to generate alarms when critical events are logged. OpManager uses WMI to fetch the details of these logs and hence you need to provide the log on details of a user with administrative privilege to connect to the Windows machine.
You can view the list of all events monitored by OpManager, by clicking **Event Log Rules** under the **Admin** tab.

- Monitoring Windows Events in a Device
- Using the Quick Configuration Wizard
- Creating an Event Log Monitor
- Monitoring Custom Event Logs

Monitoring Windows Events in a Device

To monitor Windows events, you need to associate the event log monitors with the device. To do so, follow the steps given below:

1. Go to the device snapshot page.
2. From the **Actions** menu, click **Event Log Rules**.
3. Select the event logs to be monitored in the device.
4. Change the **Polling Interval** if necessary. During each poll, the selected event logs are compared with the events logged in the device and for the matching events, alarms are generated.
5. Click **Save** to save the changes.

Using the Quick Configuration Wizard

Alternatively, you can associate an event log rule with many devices at a time using Quick Configuration wizard.

1. From the Admin tab, select Quick Configuration Wizard.
2. Select the option **Associate Event log rules to several devices** and click Next.
3. Select the log file from the displayed list.
4. Select any one rule from the list of rules shown. Click Next.
5. Select the devices on which you want to monitor the event logs from the column on the left and move them to the right.
6. Click Finish. The event log monitor is associated to the selected devices.

Creating an Event Log Monitor

To create an event log monitor, follow the steps given below:

1. Under the **Admin** tab, click **Event Log Rules**.
   In this page, you can see the rules supported by OpManager. They are categorized into Applications, Security, System, DNS Server, File Replication Service, and Directory Service. You can add the event logs that you want to monitor under any of these categories.
2. Click **New Rule** under any one of the categories to add a rule in it.
   Entries to all the fields except Rule Name are optional. Event ID is a required field to identify the event but can be left empty in few exceptional cases, such as you want to monitor all events that are of the Event Types, say, error or information. Here the filter will be based on the Event Type.
   1. Type a unique **Rule Name**.
   2. Enter the **Event ID** to be monitored. This is the unique identifier for the event logs.
   3. Enter the event **Source**. This is the name of the software that logs the event.
   4. Enter the event **Category**. Each event source defines its own categories such as data write error, date read error and so on and will fall under one of these categories.
   5. Type the **User** name to filter the event log based on the user who has logged on when the event occurred.
   6. Choose the **Event Types** to filter the event logs based on its type. This will typically be one among Error, Warning,

Information, Security audit success and Security audit failure.

7. Enter the string to be compared with the log message. This will filter the events that contains this string in the log message.
8. By default OpManager raises an alarm if the event occurs. However, you can configure the no. of consecutive times the event can occur within the specified no. of seconds, to raise an alarm.
9. Choose a severity for the alarm generated in OpManager for this event.

3. Click **Add Rule** to save the event log rule.

Monitoring Custom Event Logs

You can monitor event logs under a custom category too. Some applications log the events in a new category other than the default System/Applications/Security category. You can now configure rules in OpManager to parse the events in such custom categories and trigger corresponding alerts in OpManager. Here are the steps:

1. Go to Admin > Event Log Rules > Add Custom Event log (you will find this option on the top right corner on this screen).
2. Select a device from which you can query for the event categories and hit **Query Device**. The custom logs in the selected device are listed. As an alternative, you can add custom events category and define rules.
3. After you add the custom event category, you will find the category listed under Admin > Event Log Rules. Go on to add new rules to parse the events falling under this category.

You can now associate the rules (default or custom event logs) to the required devices.

Monitoring URLs for Availability

You can configure OpManager to monitor your Web sites. Many business enterprises require continuous monitoring of their Web sites, as the failure of these sites might have an impact on the business.

You can monitor global URLs, such as www.yahoo.com and www.manageengine.com.com or URLs in a server, such as http://192.168.4.11/index.html, http://web and so on.

You can perform a content match on these URLs and confirm their availability. Further, for pages that require a form submit, such as user name and password, you can provide these details and verify the availability of the next page.

Note: If a proxy server is configured in your network, make sure to provide its details in the Proxy Server Settings page of OpManager. Refer to Configuring Proxy Server Settings for steps to do this. This is required for monitoring any URL in a proxy-enabled LAN.

Configuring a global URL monitor

To configure a global URL monitor, follow the steps given below:

1. Go to **Admin**-> **URL Monitor** -> **Add URL**.
2. Select **URL** radio button to configure a URL monitor. This is selected by default.
3. Enter a name to the URL monitor in the **URL Monitor name** field.
4. Type the **URL address** to be monitored.
5. Type the **Monitoring Interval** and the value of **Timeout** in the respective fields.
6. Enter the number of times the URL can go down consecutively before raising an alert.
7. Type the string (max. 250 characters) to be compared with the contents of the monitored Web page in the Match Content filed. Click on the Check Now button to instantly verify the correctness of the given details.
8. Select between **Get** and **Post**, the methods for any HTTP/HTTPS-based URLs. This is required because certain URLs cannot be accessed using a Get request.
9. Type the request parameters and their values in the form <parameter name>=<value>, if any, to know the actual availability of the URL. Note that you can enter only one parameter in a line.
10. Configure the user name and password for authorization. This will be required in the pages where you need to log-on and test the availability of the host.
11. Select the required notification profile type and click **Add** button to associate it with this monitor.
12. Click **OK** to add the URL monitor.

Configuring URL monitors in bulk

For adding multiple URL monitors, you can import the URL monitor parameters through a csv file. The csv file must contain parameters like Monitor name and URL to be monitored. It can also have additional parameters like Monitoring Interval, time out, match content, profile name and device name. Username and password fields can also be added if the URL needs authorization. Make sure you provide the exact header name and follow the same format provided in the sample file.If the values are not provided for the additional parameters in csv file, the default values will be taken.

In the sample file, you can find a field named Device Name. It is used for monitor the URL from that device. The device should be either Servers or Domain Controllers. If this field is added in the csv file, the URL will be directly added to the device snapshot page. The display name of the device in OpManager or fully qualified domain name should be provided in this field.

To add multiple URL monitors, follow the steps given below:

1. Go to **Admin**-> **URL Monitor** -> **Add URL.**
2. Select **Import URLs from CSV** radio button.
3. Click on **Browse** button to import the CSV file.

4. Configure the **General properties**.
5. Click **OK** to add the URL monitors.

Viewing URL Response Time and Availability

You can get the details about the URL response time and availability in the URL snapshot page.

To view the URL snapshot, click the URL link in the Home page or Maps tab. Then click the URL whose snapshot you want to view.

Click the Availability chart to view the availability history and the URL downtime/uptime chart.

Associating URL Monitors to Servers

You can add URL monitors to Servers/Domain Controllers to check the availability of the URL from those servers.

1. Go to the device snapshot page.
2. Scroll down to the Monitors section and click URL Monitors.
3. On the right, you will find a link to add the monitors. Click to add monitors
4. Configure all the values for the URL Monitor.

The configured URL is monitored for availability from that Server. You can configure to receive an e-mail or SMS when the URL monitored in a server goes down. For this, you need to create a notification profile for the 'URL is down' criteria and associate it to the server.

To add URL monitors to Servers/Domain Controllers in bulk, click here.

Adding Syslog Rules

Syslog is a client/server protocol that sends event notification messages to the syslog receiver. These event notification messages (usually called as syslog messages) help in identifying the authorized and unauthorized activities like installing software, accessing files, illegal logins etc. that take place in the network. In OpManager Syslog rules helps in notifying you if some particular syslog messages such as kernel messages, system daemons, user level messages etc. are sent by the devices.

Apart from the pre-defined syslog rules you can also add any number of syslog rules. Here are the steps to add a syslog rule:

1. Go to **Admin**-> **Syslog Rules**.
2. Click on the **Actions** drop down menu and select **Add New Rule**. Add Syslog Rules window opens.
3. Enter a unique **Rule Name**.
4. Enter a brief **Description** about the rule.
5. Select a **Facility**. Facility refers to the application or the OS that generates the syslog message. By default "Any" is selected.
6. Select the required **Severity**.
7. Enter the text that needs to be verified for matching. Note: Regex is supported for this field.
8. Select the **Alarm Severity**.
9. Enter the **Alarm Message**.
10. Click the **Advanced** button to configure advanced (threshold) rules. This is optional.
    1. **Number of Occurrences**: Enter the count of the number of consecutive times OpManager can receive syslog message from a device before raising an alert.
    2. **Time Interval (seconds)**: Enter the time interval that should be considered for calculating the number of occurrences.

       To clear or rearm the event:
    3. Select the **Facility Name**.
    4. Select the **Severity**.
    5. Enter the **Matching Text**.
    6. Click **Save**.
11. Click **Save**.

Configuring Syslog Ports

OpManager receives the syslog packets via the default syslog port 514. However, if required you can configure additional ports in OpManager to receive the syslog packets. To configure additional ports, follow the steps given below:

1. From **Admin** tab, click **Syslog Rules**.
2. Click on the **Actions** drop down menu and select **Syslog Port**.
3. Enter the port number(s) separated by a comma.
4. Click **OK**.

Monitoring Syslog Packets

Syslog viewer allows you to ensure whether OpManager receives the syslog packets sent by the devices. Here are the steps to view the list of the devices that send the syslog packets:

1. From **Admin** tab, click **Syslog Rules**.
2. Click on the **Actions** dropdown menu and select **Syslog Viewer**.

The syslog packets sent by the devices to OpManager are listed. You can also filter the syslog packets by device and port.

Filtering Syslog packets

1. Enter the device's IP address in the **Source IP field**.
2. Enter the **port** number via which OpManager receives the syslog packets.

Viewing Syslog Flow Rate

To view the flow rate of the syslog packets,

1. Go to **Admin**-> **Syslog Rules**.
2. Click on the **Actions** dropdown menu and select **Flow Rate**.

The flow rate of the Syslog packets are displayed.

Hardware Health Monitoring

Monitor the hardware health of key device parameters such as temperate, voltage, power, fan speed, status of processors, disk arrays, etc. of VMware, HP, Dell and Cisco systems and get alerted if they violate pre-defined thresholds.

Collecting Hardware Health Data

OpManager uses SNMP to monitor and collect the hardware health status of servers, routers & switches. In-case of VMware, the vSphere API is used to collect sensor data.

The hardware health monitors are associated automatically whenever you add a device with proper SNMP credential. If you encounter any problem associating the hardware health monitors, then check for the correct SNMP credentials or contact our support team.

Reporting of Hardware Health:

OpManager provides historical reports on the status of hardware health which can be scheduled based on user needs.

OpManager - Hardware Health Monitoring Video:

Workflow

OpManager's IT automation workflows are code-free and out-of-the-box offers predefined checks and actions. It includes an agile and flexible drag-n-drop workflow builder. Workflow helps you:

- Initiate IT workflow on network faults or on a routine basis
- Manage Services, Processes, Files and Folders of Windows servers and desktops
- Record the IT workflow procedures as an XML and ensure structured practices across IT

OpManager also offers log reports of executed workflows for future analysis.

Checks and actions available in Workflow

Click here to know the conditions and actions available in Workflow.

Workflow Tasks

Tasks are are nothing but checks and actions that help you automate repeated IT actions.

Checks:

Checks are if-else condition based. If the condition is passed/satisfied, the workflow executes the set of actions associated on the success part, executes the other set of actions associated on the failure part. Example: Consider that you have created a workflow with Test a Service, Send Mail, and Start a Service tasks. Send Mail is associated on the success part of Test a Service, and Start a Service is assocated on the part. If the service is running, workflow executes Send Mail task to notify the admin that the service is running, else executes Start a Service task to start the service.

Actions:

An action just performs the said activity. Tasks such as start a service, delete file, reboot system are action tasks. If an action task is executed successfully, workflow executes the next successive task. If an action task fails, action task associated on the failure part is executed. Example: Consider that you have created a workflow with 2 action tasks - Start Process and List All Process. List All Process is associated to the success part of the Start Process task. When the workflow is executed, in case if the Start Process task is failed, workflow looks for the task associated on the failure section. If no task is found, executes the task in the success section i.e., List All Process.

Conditions and Actions available in Workflow

Device	
Checks	**Description**
DNS Lookup	Executes a DNS lookup command on the end device.
Ping Device	Sends ICMP packets to the end device.
Trace Route	Executes a trace route command on the end device.
Actions	
Add a Time Delay	Adds a delay to the execution of an action
Reboot System	Reboots the system
Shut Down System	Shuts down the system
Windows Service	
Check	
Test a Service	Tests whether a service is running or not.
Actions	
Get Active Services	Provides a list of service that are currently running.
Pause a Service	Pauses a service.
Restart Service	Restarts a service.
Resume a Service	Resumes a service.
Start a Service	Starts a service.
Stop a Service	Stops a service.
Process	
Check	
Test a Process	Test whether a process is running or not.
Actions	
List All Processes	Lists all the processes that currently running.
Processes by Disk Read	Lists processes by Disk Read.
Processes by Disk Write	Lists processes by Disk Write.
Processes by Memory Usage	Lists processes by Memory usage.
Processes by CPU Usage	Lists processes by CPU usage.
Start Process	Starts a process.
Stop Process	Stops a process.

HTTP & FTP	
Check	
Check URL	Test the availability of a URL.
Actions	
FTP Delete File	Deletes a file via FTP.
FTP Move File	Moves a file within the same remote device via FTP.
FTP Rename File	Renames a files via FTP.
FTP Upload File	Writes the given content in a file (.txt) and uploads it to the remote device via FTP.
HTTP Post Data/Result	Posts the output received upon querying an URL, in the workflow logs.
File	
Checks	
Check File	Checks the availability of a file.
Get File Size	Gets the size of a file.
Actions	
Compress Files	Files are compressed with Windows Compression.
Compress Older Files	Files which are not used for a long time are compressed with Windows Compression. You can configure the age of the files.
Copy File	Copies file to another directory within the same device.
Delete File	Deletes a file.
Delete Older Files	Deletes the files which are not used for a long time. Also deletes older files in sub folders. You can configure the age of the files.
Move File	Moves the files to another directory within the same device.
Move Older Files	Moves the files which are not used for a long time to another directory within the same device. You can configure the age of the files.
Rename File	Renames a file.
Uncompress File	Uncompresses a file.
Folder	
Checks	
Check Drive Free Space	Checks for free space available in a drive.
Get Folder Size	Gets the size of a folder.
Actions	
Compress Folder	Compresses a folder.
Copy Folder	Copies the folder to another local directory.
Create Folder	Creates a folder.
Delete Folder	Deletes a folder.
List Files	List the files available in a folder.
Move Folder	Moves a folder to another location.
Rename Folder	Renames a folder.
Uncompress Folder	Uncompresses a folder.
VMware	
Actions	
Power Off VM	Turns off the power to a VM.
Power On VM	Turns on the power to a VM.
Reboot Guest OS	Restarts a VM.
Refresh Datastore	Refreshes the datastore.
Reset VM	Resets a VM abruptly.

Shut Down Guest OS	Shuts down a VM.
Stand by Guest OS	Puts a VM in the Stand By mode.
Suspend VM	Suspends a VM.
OpManager	
Check	
Check Device Status	Checks the availability status of a device.
Actions	
Acknowledge Alarm	Acknowledges an alarm.
Add Alarm Note	Adds a note to an alarm.
Clear Alarm	Clears an alarm.
Delete Alarm	Deletes an alarm.
Exit Maintenance	Moves the device under maintenance mode to normal.
Generate Alarm	Generates an alarm in OpManager.
Place on Maintenance	Puts the device on maintenance mode.
Rediscover Device	Rediscovers a device.
Unacknowledge Alarm	Unacknowledges an alarm.
External Actions	
Actions	
Execute Another Workflow	Executes another workflow as an action.
Execute Linux Script	Executes a script on the end Linux devices.
Execute Windows Script	Executes a script on the end Windows devices.
Log a Ticket (Remedy)	Creates a ticket in BMC Remedy.
Log a Ticket (SDP)	Creates a ticket in ManageEngine ServiceDesk Plus.
Send Email	Sends a notification via Email. Ensure that you have configured Mail server settings.
Send Popup Message	Sends a notification via a pop-up on the end device. At present Workgroup devices alone are supported.
Send SMS	Sends a notification via SMS. Ensure that you have configured SMS server settings.

DNS Lookup:

DNS Lookup executes a DNS lookup command on the end device and provides its status.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device. If no device is selected, it will be executed on the device selected in the Info tab.

Ping Device:

Sends ICMP packets to test whether the device is responding.

Parameter	Description
Name	Display name for the task
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Number of requests	Number of ping requests you want to send.
Packet Size	Size of the ping packets.
Timeout	Timeout interval for the ping requests.
Retries	Number of retries for the ping operation.

Trace Route:

Executes a trace route command on the end device.

Parameter	Description
Name	Display name for the task
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device.

Add a Time Delay:

Adds a delay to the execution of the subsequent operation.

Parameter	Description
Name	Display name for the task.
Duration	Time delay to carry out the subsequent task. You can configure time delay in hours, minutes, and seconds. Select the required one from the dropdown menu.

Reboot System:

Reboots a remote Windows machine.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device.

Shut Down System:

Logs off, shuts down, reboots or powers off a remote Windows device forcefully.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device. You can also log off by selecting the Log Off action from the dropdown.
Options	Select the action (Log off, Shut down, Reboot or Power off) that you want to carryout on the remote device.

Test a Service

Tests whether a service is running or not.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Service Name	Name of the service that you want to task whether it is running or not. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device. Supported Variable: ${Alarm.ServiceName} - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime. Note: If multiple services down alarm is triggered, this task will be executed for all those services.

Get Active Services

Provides the list of active services running in the device.

Parameter	**Description**
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.

Pause/Restart/Resume/Start/Stop a Service

Pauses/Restarts/Resumes/Starts/Stops a service.

Parameter	**Description**
Name	Display name for the task.

Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Service Name	Name of the service that you want to pause/restart/resume/start/stop. Use the dropdown menu to select the service. If the service is not listed, use the discover icon to discover the services running the device. Supported Variable: ${Alarm.ServiceName} - Select this option if you want to retrieve the service name from the alarm entity. If the workflow is triggered from the service down alarm, then this variable is replaced by the servicename from the alarm entity during runtime. Note: If multiple services down alarm is triggered, this task will be executed for all those services.

Test a Process

Tests whether a process is running or not.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Process Name	Name of the process that you want to test. Either you can enter the process name right away (Eg.:mysqld-nt.exe) or you can use the select icon to select the process from the remote devices.
Path	This field is optional. If you want to match the path also, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. Eg.: C:Program FilesMySQLMySQL Server 5.0binmysqld-nt.exe
Arguments	This field is also optional. If you want to match the arguments, then check the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. Eg.: --defaults-file="my.ini"

List All Processes/Processes by Disk Read/Processes by Disk Write/Processes by Memory Usage/Processes by CPU Usage

Provides the list of active services, processes by disk read/disk write/Memory usage/CPU usage.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.

Start Process

Starts a process.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Start Directory	The directory from where you want to execute the process.
Process Command	Command to start the process.

Stop Process

Stops a process running on a device.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select devices icon to select the device.
Process Name	Name of the process that you want to test. Either you can enter the process name right away (Eg.:mysqld-nt.exe) or you can use the select icon to select the process from the remote devices.

Path	This field is optional. If you want to match the path while terminating the process, then check the checkbox near path field and specify the full executable path with process name. Otherwise leave this field empty. Ex: C:Program FilesMySQLMySQL Server 5.0binmysqld-nt.exe Note: If the checkbox is unchecked and multiple instance of process is running with the same name, all the processes will be terminated.
Arguments	This field is also optional. If you want to match the arguments when terminating the process, select the checkbox near arguments field and specify the arguments. Otherwise leave this field empty. Ex: --defaults-file="my.ini" Note: If the checkbox is unchecked and multiple instance of process is running with the same name, all the processes will be terminated.

Check URL

Check whether the URL for its availability.

Parameter	Description
Name	Display name for the task.
URL Address	Address of the HTTP URL that has to be queried. Supported Variables : ${Alarm.URLAddress} - will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.
Form Method: Get or Post	OpManager tests the URL via Get or Post method. Select the appropriate condition.
Search and Match Content	The content specified here is verified for its presence in the web page.
Timeout	Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.
URL Authorization Details	Provide the username and password for URLs that require authentication.
Check Now	Checks whether the URL is accessible with the entered details.

FTP Delete File

Deletes a file via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
File Name	Name of the file to be deleted. Enter the file name with the path.

FTP Move File

Move a file to another directory within the same system via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.

File Name	Name of the file to be moved. Enter the file name with the path.
Destination Folder	Destination folder where the file to has to be moved. Enter the path.

FTP Rename File

Renames a file via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
Source File	Name of the file to be renamed. Enter the file name with the path. Eg.:/root/OpManager/backup/Backup_DB.zip
New Name	New name for the file. Eg.: Backup_DB_Old.zip

FTP Upload File

Writes the given content in a file (.txt) and uploads it to the remote device via FTP.

Parameter	Description
Name	Display name for the task.
FTP Server	Name of the FTP Server. You can enter the ftp server name directly or use '${DeviceName}' variable. '${DeviceName} will be replaced with the name device selected in the Info tab, during the workflow execution.
FTP Username	Username of the FTP server.
FTP Password	Password to connect to the FTP server.
Directory	Directory where the file has to be uploaded.
Content	Content/value that has to be uploaded

HTTP Post Data/Result

Posts the output received upon querying an URL, in the workflow logs.

Parameter	Description
Name	Display name for the task.
URL Address	Address of the HTTP URL that has to be queried. Supported Variables : ${Alarm.URLAddress} - will retrieve the URLAddress from the alarm entity, if workflow is triggered through alarm. Otherwise nothing will happen.
Form Method: Get or Post	OpManager tests the URL via Get or Post method. Select the appropriate condition.
Search and Match Content	The content specified here is verified for its presence in the web page.
Timeout	Timeout interval for the URL. Default value is 25 seconds. Click on check now button to verify the URL.
URL Authorization Details	Provide the username and password for URLs that require authentication.
Check Now	Checks whether the URL is accessible with the entered details.
Post Data	The content specified here will be displayed in the execution logs. Supported Variables : ${URLAddress} - will replace the address specified in the URL Address field. ${Result} - will replace the response obtained from the URL Address.

Check File

Checks the existence of a file in the specified path.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be checked for its existence. Specify the file name with its path.

Get File Size

Checks the file for its size and execute tasks accordingly.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to checked for its size. Specify the file name with its path.
File Size	The size of the file is compared with the value specified here. According to the condition (greater or lesser than) selected the actions are executed.

Compress File/Delete File

Compresses a file with Windows Compression/Deletes a file.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be compressed/deleted. Specify the file name with its path.

Compress Older Files/Delete Older Files

Compresses older files with Windows Compression/deletes older files.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Folder that contains the old files. Specify the folder path. Note: Delete older files option, deletes the older files in the sub folders also.
Files Older Than	Files older than the specified number of months/days/hours are compressed/deleted.

Copy File/Move File

Copies/moves a file from one folder to another within the same computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be copied/moved to another folder. Specify the file name with its path.You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.
Destination Folder	Name of the folder where the file has to be pasted/moved. Specify the folder path.

Move Older Files

Moves files that match the age specified to another folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source Folder	Folder that contains the old files. Specify the folder path.
Destination Folder	Folder to which the old files have to be moved to.
Files Older Than	Files older than the specified number of months/days/hours are moved.

Rename File

Renames a file.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source File Name	Specify the source file name to be renamed Eg.: C:Program FilesOpManagerbackupBackup_DB.zip
New Name	New name for the file. Eg.: Backup_DB_Old.zip

Uncompresses File

Uncompresses a file that had been compressed with Windows Compression.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the file that has to be uncompressed. Specify the file name with its path. You can use the wild card character * (eg.: stderr*.txt) to do the action on all the files. You can also enter multiple files separated by a comma.

Check Drive Free Space

Checks the free space available in a drive.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Drive Name	Name of the drive that has to checked for free space.
Drive Size	The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.

Check Folder Exists

Checks the existence of a folder in the specified path.

Parameter	Description
Name	Display name for the task.

Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
File Name	Name of the folder that has to be checked for its existence. Specify the folder path.

Get Folder Size

Checks the free space available in a drive.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to checked for its size.
Folder Size	The size of the drive is compared with the value (GB/MB/KB) specified here. According to the condition (greater or lesser than) selected the actions are executed.

Compress /Uncompress/Delete Folder

Compresses/uncompresses/deletes a folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Folder that has to be compressed/uncompressed/deleted. Specify the folder path.

Create Folder

Creates a folder in the computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to be created. Specify the folder name with its path.

Copy Folder/Move Folder

Copies/moves a folder to another folder within the same computer.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder that has to be copied/moved to another folder. Specify the file name with its path.
Destination Folder	Name of the destination folder where the source folder has to be pasted/moved. Specify the folder path.

List Files

List the files available in a folder.

Parameter	Description

Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Folder Name	Name of the folder whose files has to be listed. Specify the folder path.

Rename Folder

Renames a folder.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Source Folder	Specify the source folder name to be renamed Eg.: C:OpManagerlogs
New Name	New name for the folder. Eg.: logs_old

Add Alarm Note

Adds note to an alarm.

Parameter	Description
Name	Display name for the task.
Note	Note that has to be added to the alarm. Supported Variables : ${Result} - will be replaced with the previously executed task's result.

Generate Alarm

Generates an alarm in OpManager.

Parameter	Description	
Name	Display name for the task.	
Source	Note that has to be added to the alarm. Supported Variables : ${Result} - will be replaced with the previously executed task's result.	
Severity	Select the severity of the alarm.	
Message	Message that you want to display in the alarm.	
Alarm Code		Unique string used to trigger the event. Eg:-Threshold-DOWN
Entity	Uniquely identifies the failure object within the source.Events will be correlated into alarms according to the entity field. Multiple events with the same entity will be grouped as a single alarm.	
Event Type	Description of the event type	

Execute Linux Script

Execute script on remote Linux machines and retrieves the output. Depending on the input, this script will either execute from OpManager server or from remote machine. Its success/failure is decided based on its exit code. If the script returns with the exit code 0, then it is consider as success, any other value is consider as failure.

Eg.:For shell script,

exit(0) -- Success

exit(1) -- Failure

exit(-2) -- Failure

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Command Line	Specify the command used to execute the script. Eg.: sh ${FileName} ${DeviceName} arg1 Here, ${FileName} variable is a must to execute the script. OpManager will replace this variable during runtime. Supported Variables : ${DeviceName} - will replace the executing devicename during runtime. ${UserName} - will replace the device username if already given for this device. ${Password} - will replace the device password if already given for this device.
Script Body	The actual script that has to be executed.
Advanced	Click on Advanced button to configure the following fields.
Execute from Remote Machine	If this option is checked, the script is pushed to remote machine and will be executed. Otherwise it will be executed from OpManager server.
Working Directory	Specify the directory from where you want to execute the script. Supported Variables : ${UserHomeDir} - will replace the user's home directory during runtime. ${TempDir} - will replace device temp directory during runtime. Eg: /tmp
Response Timeout	Time to wait for the script to complete its execution. The default value given here is 60 seconds.

Execute Windows Script

Execute the script on remote Windows machines from OpManager server and retrieves the output. Its success/failure is decided based on its exit code.

If the script returns with the exit code 0, it is consider as success, any other value is consider as a failure.

Eg.: for VBscript:

WScript.Quit(0) -- Success

WScript.Quit(1) -- Failure

WScript.Quit(-2) -- Failure

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Command Line	Specify the command used to execute the script. Eg. : cscript ${FileName}.vbs ${DeviceName} ${UserName} ${Password} arg1 Here, ${FileName} variable is must to execute the script. OpManager will replace this variable during runtime. Supported Variables : ${DeviceName} - will replace the executing devicename druing runtime. ${UserName} - will replace the device username if already given for this device. ${Password} - will replace the device password if already given for this device.
Script Body	The actual script that has to be executed.
Advanced	Click on Advanced button to configure the following fields.

Working Directory	Specify the directory from where you want to execute the script. Supported Variables : ${UserHomeDir} - will replace the user's home directory during runtime. ${TempDir} - will replace OpManager temporary directory during runtime.
Response Timeout	Timeout interval for the response from the device for the script execution status.

Log a Ticket (Remedy)

Logs a ticket in BMC Remedy.

Parameter	Description
Name	Display name for the ticket.
From Email ID	Email ID of the sender.
Service Desk Mail ID	Email ID of BMC Remedy service desk.
Impact	Select the impact level of the ticket.
Urgency	Select the severity of the ticket.
Summary	Add summary for quick understanding of the issue reported.
Description	Describe the issue.

Log a Ticket (SDP)

Logs a ticket in ManageEngine ServiceDesk Plus. Ensure that ServiceDesk Plus is integrated with OpManager.

Parameter	Description
Name	Display name for the ticket.
Category	Select the appropriate category for the ticket.
Sub Category	Select the appropriate sub category.
Item	Select the appropriate item.
Priority	Select the priority level of the ticket.
Group	Select the group.
Technician	Select the technician to whom you want to assign the ticket.
Title	Subject of the ticket. You can use variables.
Description	Describe the issue. You can use variables.

Send Mail

Sends a mail to the email IDs specified. This is useful to notify the result/completion of a task in the workflow.

Parameter	Description
Name	Display name for the task.
From Email ID	Email ID of the sender.
To Mail ID	Email ID of of the recipients.
Mail Format	Email can be sent in plain text or html or in both the formats. Select the required format.
Subject	Subject of the email.You can use variables.
Message	Content of the email. You can use variables.

Send Popup Message

Opens a popup window with the given message on remote computers.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Message	Message that has to be displayed in the popup.

Send SMS

Sends SMS notifications to the mobile number specified. This is useful to notify the result/completion of a task in the workflow.

Parameter	Description
Name	Display name for the task.
Destination Device	Device on which the task has to be executed. Click on the select device icon to select the device or use ${DeviceName} variable. ${DeviceName} will be replaced with the name of the device that is selected in the Info-> Devices, during the workflow execution.
Message	Message that has to be sent as an SMS. Message should not exceed 160 characters.

Variables:

Variables are used to append dynamic values in a field of a task. Following are the variables:

${DeviceName} - Name of the device to which workflow has to be associated. Can be used in all fields

${WorkflowName} - Name of the Workflow that is to triggered. Can be used in all fields.

${Result} - Result of previous task.

${Alarm.ServiceName} - Name of the service for which an alarm is raised.

${URLAddress} - URL address

${Alarm.URLAddress} - URL address for which an alarm is raised.

${UserName} - Username of the device.

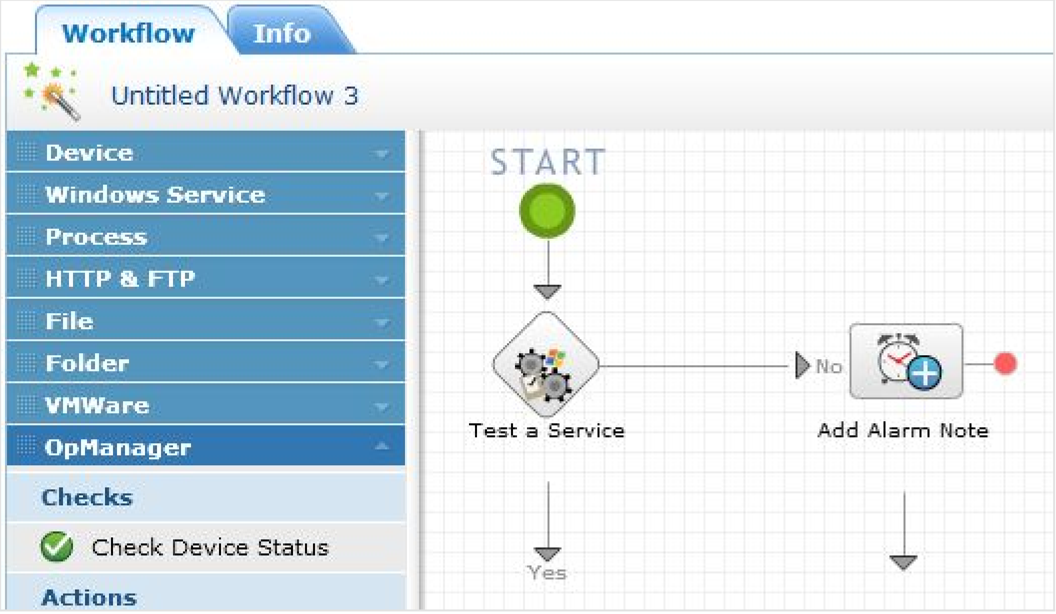
${Password} - Password of the device.

${Device.DisplayName} - Display name of the device for which an alarm is raised.

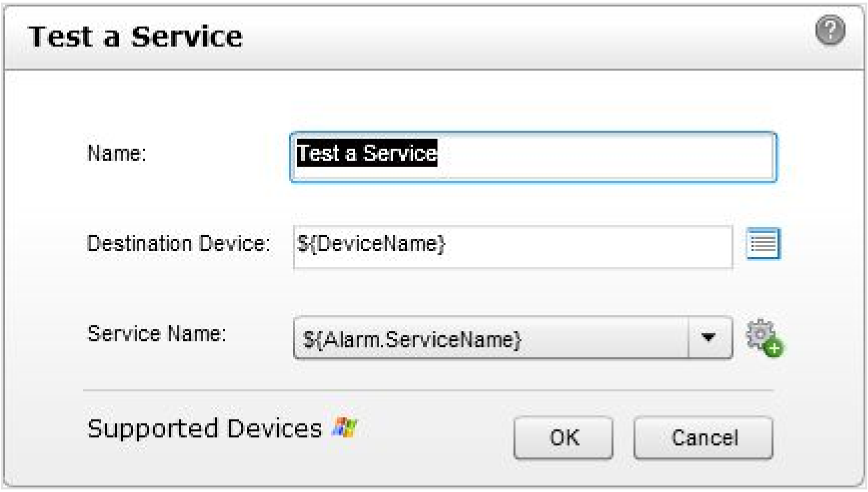
${Alarm.ProcessName} - Name of the process for which an alarm is raised.

Using Variables

Variables can be better understood with an example. Following is the workflow that has to be triggered as an action whenever a service down alarm is raised.



Task1: 'Test a service' task is created to test the service that is down. When the workflow is triggered, the variable ${Alarm.ServiceName`} is replaced with the name of the service that has gone down. ${DeviceName} is replaced with the name of device.



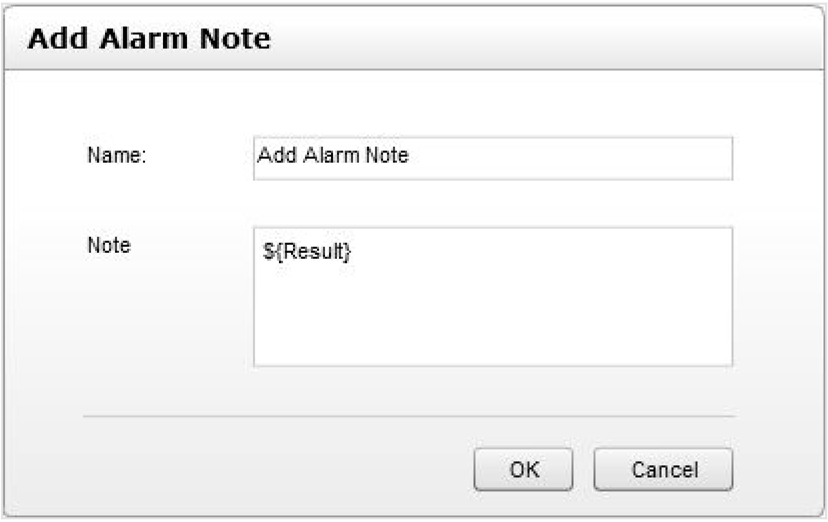
Test a Service

Name: Test a Service

Destination Device: ${DeviceName}

Service Name: ${Alarm.ServiceName}

Task 2: The result of previous task (service up or down) is added as notes to the alarm using ${Result} variable.



Add Alarm Note

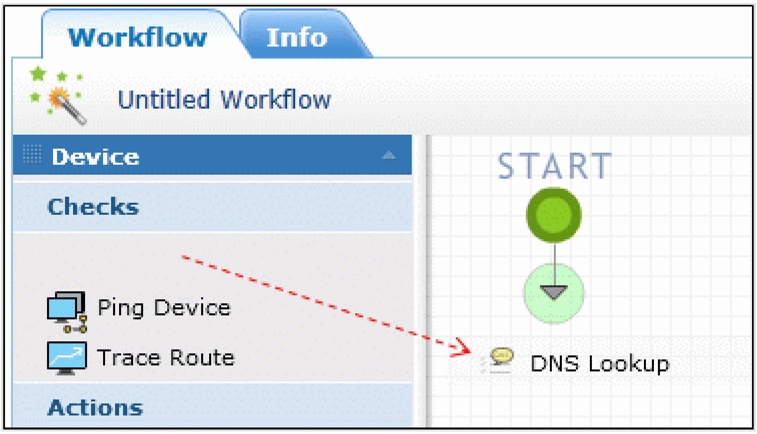
Name: Add Alarm Note

Note ${Result}

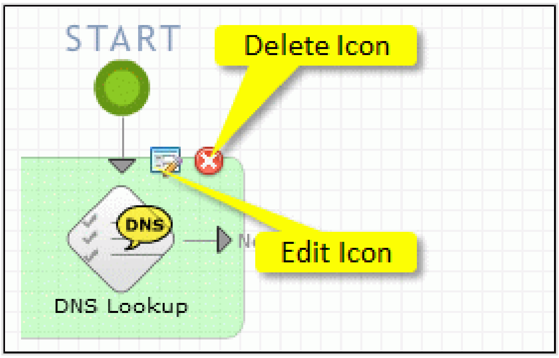
Adding a Workflow

To add a workflow, follow the steps given below:

1. Click on **Workflow tab** and select **New Workflow**.
2. Drag and drop the required conditions and actions from the left panel to editor panel.



   1. Enter a **Name** for the condition and actions.
   2. To edit or delete a condition or action, click on it and select edit or delete icon.



3. Click **Next**.
4. Enter a **Name**, **Description**, and **Tags** for the workflow.
5. Associate the workflow to the devices.
   1. Click on '**Click here to specify devices**' link corresponding to Devices tab.
   2. Select the devices in Available Devices column and move to Selected devices column. Use the search box to search the devices.
   3. Click **Update** button to associate the workflow to the devices.
6. Schedule the workflow execution. This is not required if you want this workflow to be triggered when an alarm is raised (point 7).
   1. Click on '**Click here to specify workflow schedule**' link corresponding to Schedule tab.
   2. Configure the date and time.
   3. Click **Update** button to save the schedule.
7. Configure the alarm trigger to trigger a workflow when an alarm is raised. This is not required if you want to schedule this workflow for periodical execution (point 6).
   1. Click on '**Click here to specify alarm trigger**' link corresponding to Alarm Trigger tab.
   2. Select the required criteria. Executes this workflow on the associated devices, if any of the criteria is satisfied.
   3. Define Time: Select either **Apply this profile** all time or **Apply this profile during the below mentioned time window**. Selecting the latter keeps the Workflow active only during the specified days and hours.

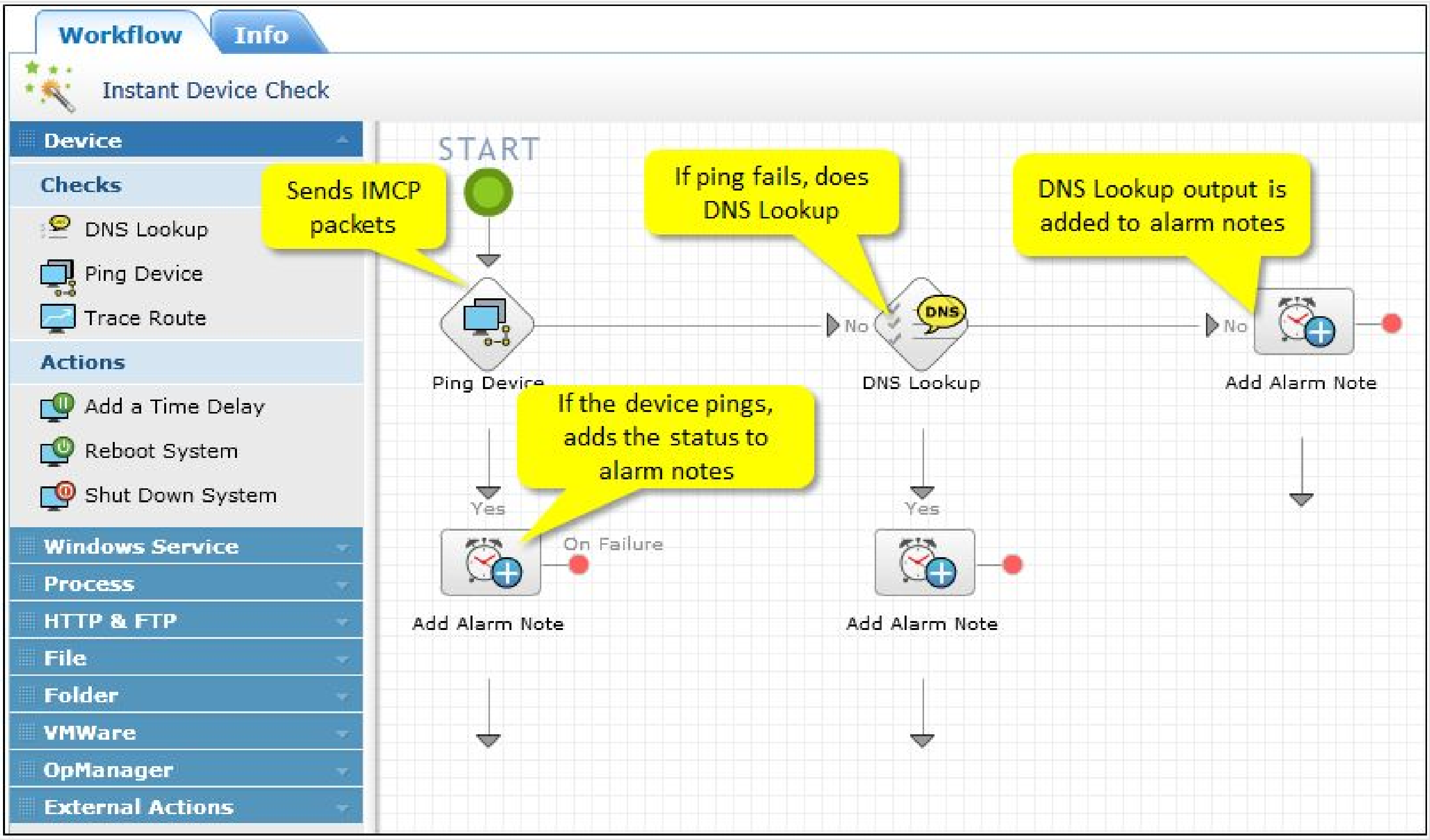
4. Delayed Trigger: If you want the workflow to be triggered at a delay, enter the delay time (in minutes). If you don't want to trigger the workflow if the alarm has been acknowledged in the mean time, you can select the 'Do not trigger if alarm is acknowledged' check box.
5. Recurring Trigger: This option helps you trigger the workflow at regular intervals, till the alarm is cleared. Enter the trigger interval and number of triggers. If you don't want to trigger the workflow repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' check box.
6. Click **Update** button.

8. Click **Save & Finish**.

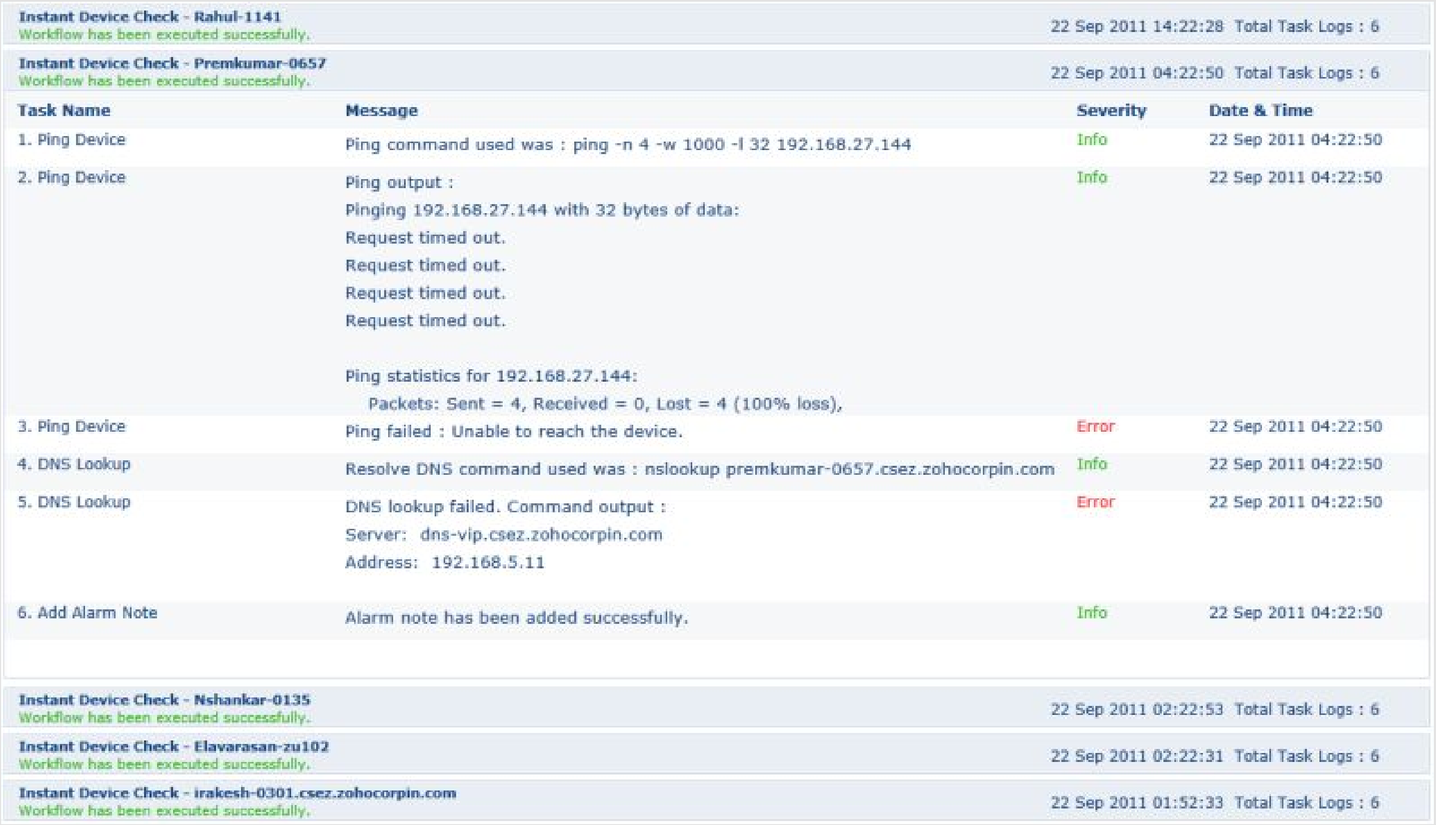
The workflow has been successfully added. It will be executed on the associated devices at the scheduled time or when any of the criteria selected is satisfied. You can check the output of the workflow in the Workflow Logs.

Sample Workflow

Following is a sample workflow which helps gets executed automatically when a device down alarm is raised. This workflow sends ping request, if passed does DNS Lookup and adds the output as notes to the alarm.



Workflow Execution Logs for the sample workflow:



Instant Device Check - Rahul-1141
Workflow has been executed successfully. 22 Sep 2011 14:22:28 Total Task Logs : 6

Instant Device Check - Premkumar-0657
Workflow has been executed successfully. 22 Sep 2011 04:22:50 Total Task Logs : 6

Task Name	Message	Severity	Date & Time
1. Ping Device	Ping command used was : ping -n 4 -w 1000 -l 32 192.168.27.144	Info	22 Sep 2011 04:22:50
2. Ping Device	Ping output : Pinging 192.168.27.144 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.27.144: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),	Info	22 Sep 2011 04:22:50
3. Ping Device	Ping failed : Unable to reach the device.	Error	22 Sep 2011 04:22:50
4. DNS Lookup	Resolve DNS command used was : nslookup premkumar-0657.csez.zohocorpin.com	Info	22 Sep 2011 04:22:50
5. DNS Lookup	DNS lookup failed. Command output : Server: dns-vip.csez.zohocorpin.com Address: 192.168.5.11	Error	22 Sep 2011 04:22:50
6. Add Alarm Note	Alarm note has been added successfully.	Info	22 Sep 2011 04:22:50

Instant Device Check - Nshankar-0135
Workflow has been executed successfully. 22 Sep 2011 02:22:53 Total Task Logs : 6

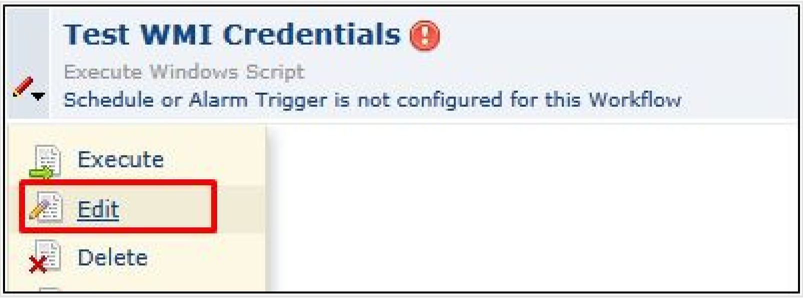
Instant Device Check - Elavarasan-zu102
Workflow has been executed successfully. 22 Sep 2011 02:22:31 Total Task Logs : 6

Instant Device Check - irakesh-0301.csez.zohocorpin.com
Workflow has been executed successfully. 22 Sep 2011 01:52:33 Total Task Logs : 6

Editing a Workflow

To edit a workflow, follow the steps given below:

1. Click on **Workflow** tab.
2. Mouseover the workflow you want to edit and click on **Edit** link.



Test WMI Credentials

Execute Windows Script

Schedule or Alarm Trigger is not configured for this Workflow

3. The workflow edit panel opens. Perform the changes you want to do and click **Next**.
4. Modify the name, description, tags, associated devices, schedule, and alarm trigger options if required.
5. Click **Save & Finish**.

Deleting a Workflow

To delete a workflow, follow the steps given below:

1. Click on **Workflow** tab.
2. Mouseover the workflow you want to edit and click on **Delete** link.
3. Click **OK** to confirm deleting the workflow.

Copying a Workflow

You can save a copy of the workflow for easy modification. To copy a workflow, follow the steps given below:

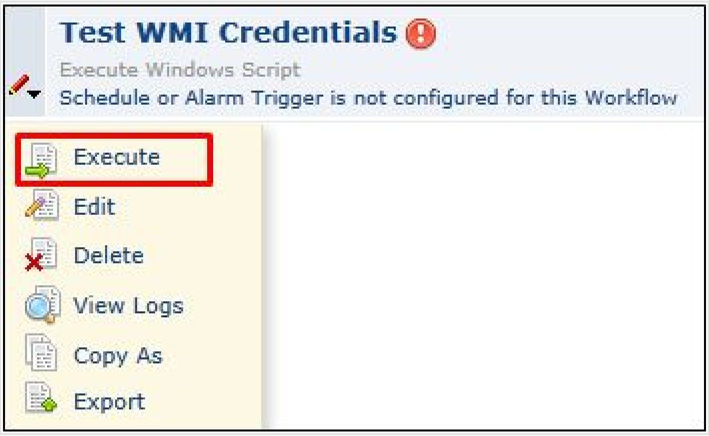
1. Click on **Workflow** tab.
2. Mouseover the workflow you want to edit and click on **Copy As** link.
3. Edit the workflow as per your requirements.

4. Click **Save & Finish**.

Executing Workflows

Before executing a Workflow, ensure that you have associated the workflow to the devices. To execute a worklow

1. Click on Workflow tab. All the created workflows are listed.
2. Mouseover the workflow you want to execute and click on Execute.



3. Description: execute workflow
4. Select the devices in the Associated Devices box and move to Selected Devices box.
5. Click Execute Now button to execute the workflow the selected devices.

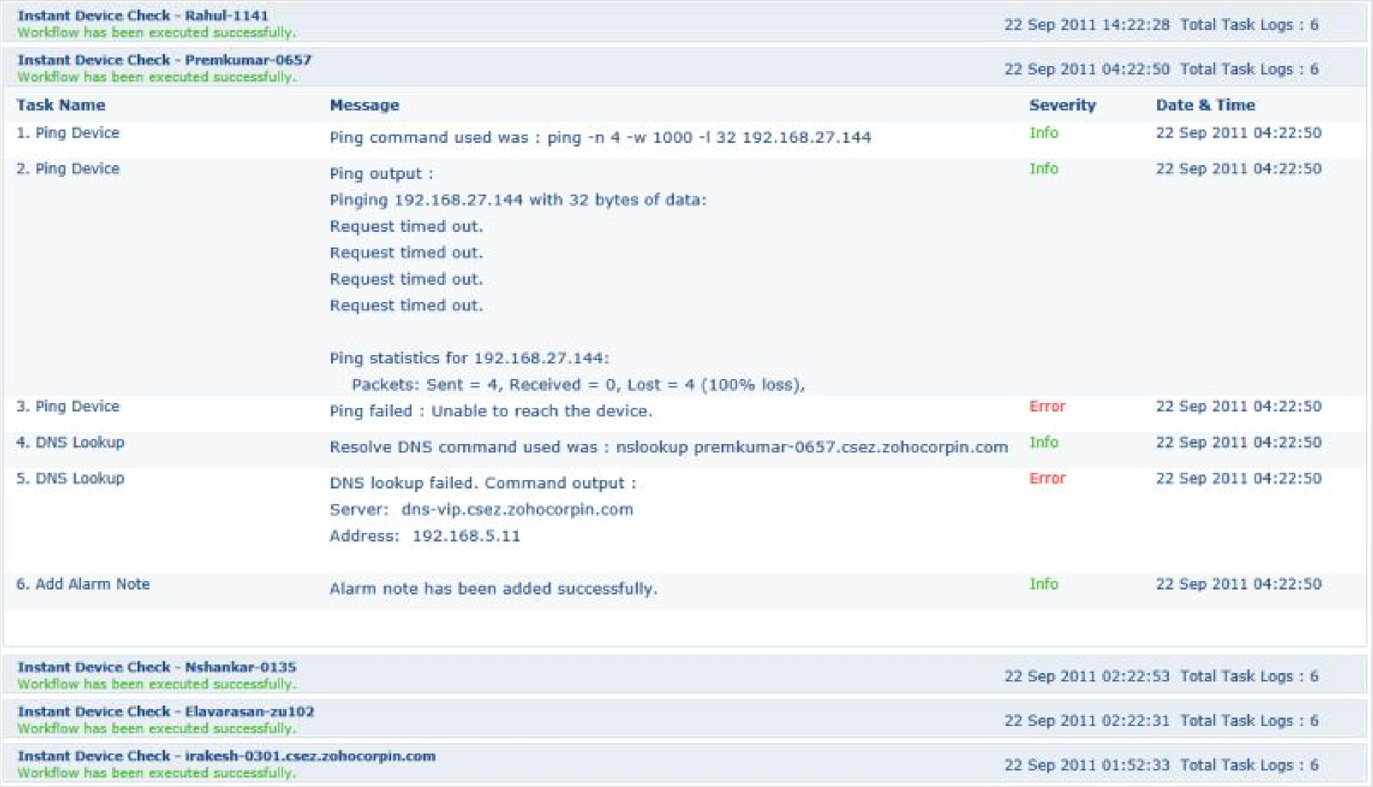
Check the output of the workflows in Workflow Logs.

Workflow Execution Logs

Workflow Logs provide the ouput of the executed workflows. It provides the result as well the data of each task that had been included in the workflow. You can also generate reports on Workflow logs [Reports-> System-> Workflow Logs].

To view Workflow logs

1. Click on Workflow tab, and select Workflow Logs. Workflow output for each of the associated device is listed along with the executed date & time and numnber of tasks.
2. Click on the required Workflow Log to view the output.



Instant Device Check - Rahul-1141
Workflow has been executed successfully. 22 Sep 2011 14:22:28 Total Task Logs : 6

Instant Device Check - Premkumar-0657
Workflow has been executed successfully. 22 Sep 2011 04:22:50 Total Task Logs : 6

Task Name	Message	Severity	Date & Time
1. Ping Device	Ping command used was : ping -n 4 -w 1000 -l 32 192.168.27.144	Info	22 Sep 2011 04:22:50
2. Ping Device	Ping output : Pinging 192.168.27.144 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.27.144: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),	Info	22 Sep 2011 04:22:50
3. Ping Device	Ping failed : Unable to reach the device.	Error	22 Sep 2011 04:22:50
4. DNS Lookup	Resolve DNS command used was : nslookup premkumar-0657.csez.zohocorpin.com	Info	22 Sep 2011 04:22:50
5. DNS Lookup	DNS lookup failed. Command output : Server: dns-vip.csez.zohocorpin.com Address: 192.168.5.11	Error	22 Sep 2011 04:22:50
6. Add Alarm Note	Alarm note has been added successfully.	Info	22 Sep 2011 04:22:50

Instant Device Check - Nshankar-0135
Workflow has been executed successfully. 22 Sep 2011 02:22:53 Total Task Logs : 6

Instant Device Check - Elavarasan-zu102
Workflow has been executed successfully. 22 Sep 2011 02:22:31 Total Task Logs : 6

Instant Device Check - irakesh-0301.csez.zohocorpin.com
Workflow has been executed successfully. 22 Sep 2011 01:52:33 Total Task Logs : 6

Severity

Each task once executed is logged with its severity for understanding its execution status. Following are the severities in Workflow:

- Info: Notifies a task has been executed successfully.
- Error: Notifies a task has been failed.
- Warning: Notifies that a task cannot be performed. Eg.: A delete file action cannot be performed when the directory does not have the specified file. In such cases, the delete file actions is marked as warning

Import/Export Workflows

OpManager saves workflows in xml format for easy sharing. You can share workflows that are created by you with OpManager community. Similarly you can use the workflow shared by peer users in the community,

Import Workflows

Workflows can be imported be local folder only. If you want to use a workflow that is shared in OpManager community, first download it on your local machine first and then follow the steps given below

1. Click on **Workflow** tab.
2. Click on **Import** link available on the top right.
3. Enter a name for the workflow.
4. Click on **Browse** button to locate the file.
5. Click on **Import** button to import the workflow into OpManager.

Export Workflows

1. Click on **Workflow** tab.
2. Mouseover the workflow you want to execute and click on **Export**.
3. Click on **Save** button to save the workflow.

Tab Customization

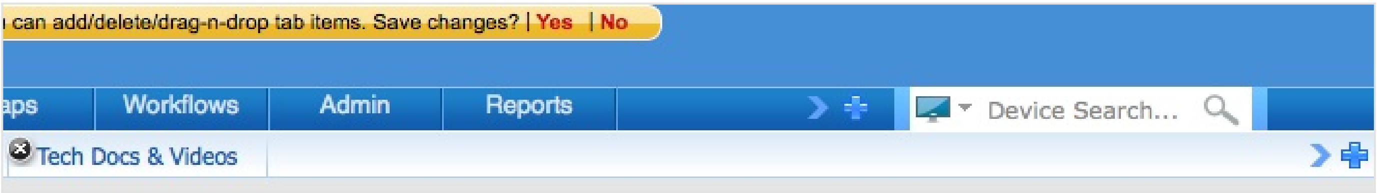
Tab customization option helps you customize/add new/delete tabs as per your requirements.

Benefits with Tab Customization:

- Create new tabs and embed graphs from other IT management tools
- Create a tab for frequently visited pages, for quick and easy navigation

Adding a new tab:

1. Mouseover **Admin** (on the top right) and click **Edit Tab**.



can add/delete/drag-n-drop tab items. Save changes? | Yes | No

2. By clicking the plus icon you can add high level as well as the sub level tabs.
   1. Enter the **Tab Name**.
   2. Select the **Type**.

      URL: URL of the OpManager page/setting/configuration/report (copy the URL by opening the web client in another tab).

      Next select how you want to open the URL i.e., in same window or as an IFrame or in a new window

      Embed: IFrame code of widgets/videos/slides
   3. Click **OK**. A new tab will be created.
3. Click **Yes** on the yellow color 'Save Changes?' notification message displayed on top of the tab.

You have successfully added a new tab.

Editing a tab:

1. Mouseover **Admin** (on the top right) and click **Edit Tab**.
2. Click on the name of the Tab that you want to edit.
3. Modify the required fields and click OK.
4. Click **Yes** on the yellow color 'Save Changes?' notification message displayed on top of the tab.

You have successfully edited a tab.

Moving a tab:

1. Mouseover **Admin** (on the top right) and click **Edit Tab**.
2. Click on the tab, drag and drop to the required spot.
3. Click **Yes** on the yellow color 'Save Changes?' notification message displayed on top of the tab.

You have successfully moved a tab to a new spot.

Deleting a tab:

1. Mouseover **Admin** (on the top right) and click **Edit Tab**.
2. Click on the tab that you want to delete. A delete icon appears on the tab.
3. Click on the delete icon.
4. Click **Yes** on the yellow color 'Save Changes?' notification message displayed on top of the tab.

You have successfully deleted a tab.

Resetting the Tabs:

If you want to revert back to the default tab settings

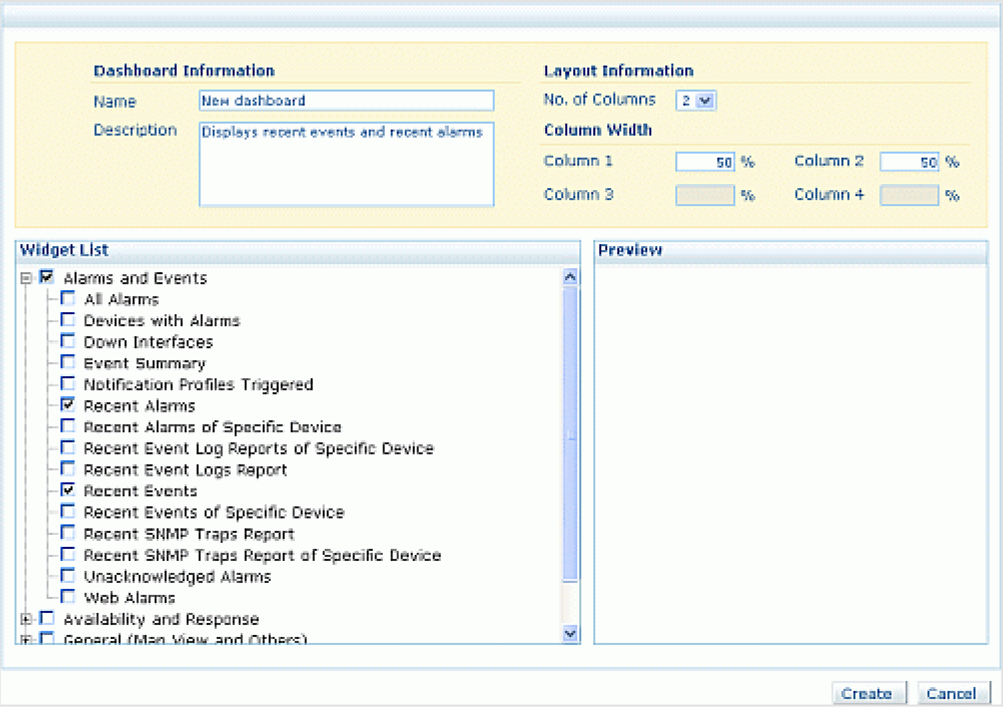
1. Mouseover **Admin** (on the top right) and click **Reset Tab**.
2. Click **OK** on the confirmation pop-up window.

All the customizations done by you will be reset to the default tab settings.

Create New Dashboard

Customizing Dashboard feature in OpManager helps you to create your own dashboard and view the desired performance metrics, reports etc at-a-glance. To create a New Dashboard follow the steps given below:

1. From **Dashboards** tab, click on **Action** drop down menu and select **New Dashboard**. Create New Dashboard window opens [screen shot given below].



Dashboard Information

Name: New dashboard

Description: Displays recent events and recent alarms

Layout Information

No. of Columns: 2

Column Width

Column 1: 50 % Column 2: 50 %

Column 3: % Column 4: %

Widget List

- ☑ Alarms and Events
  - □ All Alarms
  - □ Devices with Alarms
  - □ Down Interfaces
  - □ Event Summary
  - □ Notification Profiles Triggered
  - ☑ Recent Alarms
  - □ Recent Alarms of Specific Device
  - □ Recent Event Log Reports of Specific Device
  - □ Recent Event Logs Report
  - ☑ Recent Events
  - □ Recent Events of Specific Device
  - □ Recent SNMP Traps Report
  - □ Recent SNMP Traps Report of Specific Device
  - □ Unacknowledged Alarms
  - □ Web Alarms
- □ Availability and Response
- □ General (Map View and Others)

2. **Name**: Enter a unique name for the dashboard.
3. **Description**: Brief description about the dashboard.
4. **No. of Columns**: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
5. **Column 1, Column 2, Column 3 & Column 4**: Enter the width of the columns in terms of percentage.
6. **Widget List**: Select the Widgets that are to be displayed on the dashboard.
7. **Preview**: Displays the preview of the dashboard.
8. Click **Create** button.

A new dashboard is created and listed under the Dashboard drop down menu that is available in the Home page.

Adding New Widgets

To add a new widget to a dashboard follow the steps given below:

1. Mouse-over **Dashboards** tab and click on name of the **Dashboard** to which you want add widgets.
2. Click on **Actions** drop down menu and select **Add Widgets**.
3. Select the Widget(s) that you want add to the dashboard.
4. Click **Add** button to add the selected widget(s) to the dashboard.

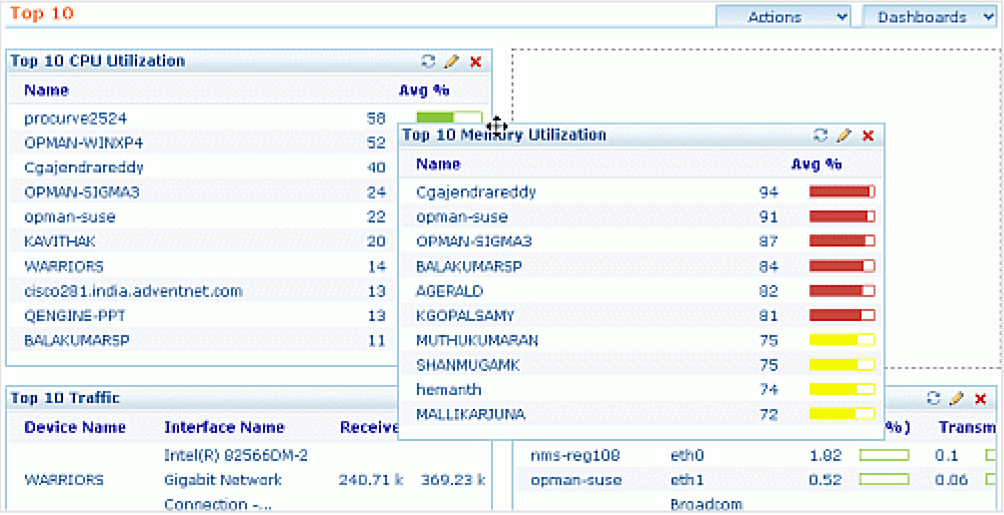
Editing Widgets

To modify the existing widgets go through the steps given below:

1. Click on **drop-down** icon available on the widget box and select **Edit**.
2. Modify the required fields.
3. Click **Submit** to effect the changes.

Moving Widgets

OpManager allows you to move the widgets to different locations within the dashboard. To move a particular widget to a different location, click on the widget name (without releasing the click) and drag the widget to the required location.



Top 10 CPU Utilization

Name	Avg %
procurve2524	58
OPMAN-WINXP4	52
Cgajendrareddy	40
OPMAN-SIGMA3	24
opman-suse	22
KAVITHAK	20
WARRIORS	14
cisco281.india.adventnet.com	13
QENGINE-PPT	13
BALAKUMARSP	11

Top 10 Memory Utilization

Name	Avg %
Cgajendrareddy	94
opman-suse	91
OPMAN-SIGMA3	87
BALAKUMARSP	84
AGERALD	82
KGOPALSAMY	81
MUTHUKUMARAN	75
SHANMUGAMK	75
hemanth	74
MALLIKARJUNA	72

Top 10 Traffic

Device Name	Interface Name	Receive	
WARRIORS	Intel(R) 82566DM-2 Gigabit Network Connection -...	240.71 k	369.23 k

		%)		Transm
nms-reg108	eth0	1.82		0.1
opman-suse	eth1 Broadcom	0.52		0.06

The widget is now moved to the new location. The widget that is near the old location occupies the old location automatically.

Embedding Widgets

Embed widgets as iframes in your website and access it without logging into OpManager. To get the iframe snippet code:

1. Click on **drop-down** icon available on the widget box and select **Embed**.
2. Copy the iframe snippet code and paste it on the required html page.

Deleting Widgets

To delete a widget go through the steps given below:

1. Click on the **drop-down** icon available on the widget box and select **Delete**. A confirmation window pops up.
2. Click **OK** to confirm deleting.

Setting a Custom Dashboard as the Default Dashboard

To set a custom dashboard as your default dashboard, follow the steps given below:

1. Mouse-over **Dashboards** tab and select the **Dashboard** which you want to set as the default dashboard.
2. Click on **Actions** drop down menu and select **Set as Default**.

The dashboard will be displayed whenever you log-in to OpManager or access the Dashboards tab.

Editing Dashboard Layout

To modify the existing dashboard layout follow the steps given below:

1. Mouse-over **Dashboards** tab and select the **Dashboard** whose layout has to be changed.
2. Click on **Actions** drop down menu and select **Edit Layout**.
3. **Name**: Enter a unique name for the dashboard.
4. **Description**: Brief description about the dashboard.
5. **No. of Columns**: Select the number of columns that you want to have in the dashboard. By default the number of columns is 2.
6. **Column 1, Column 2, Column 3 & Column 4**: Enter the width of the columns in terms of percentage.
7. Click **Modify** to effect the changes on the dashboard.

Delete Dashboard

To delete a dashboard follow the steps given below:

1. Mouse-over **Dashboards** tab and click on the name of the **Dashboard** that you want to delete. That particular dashboard opens.
2. Now click on **Actions** menu and select **Delete**. A confirmation window pops-up.
3. Click **OK** to confirm deleting.

Note: Default dashboard cannot be deleted.

Adding New CCTV

CCTV helps you view only the required dashboards repeatedly at required intervals. To add a new CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click **Add CCTV**. Create CCTV window opens.
3. **CCTV Name**: Enter a unique CCTV name.
4. **Description**: Enter a brief description about this CCTV.
5. **Refresh Interval**: Select the interval required to switch over to the next dashboard.
6. Select the desired dashboards that you want to include in this CCTV.
7. Click **Save**.

A new CCTV has been added.

Viewing CCTV

To view a CCTV, mouse-over the **Dashboards** tab and click on the name of the CCTV that you want to view. That particular CCTV opens in a new window.

Editing a CCTV

To edit a CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click the edit icon that is corresponding to the name of the CCTV that you want to edit.
3. Make the necessary changes.
4. Click **Save** to effect the changes.

Deleting a CCTV

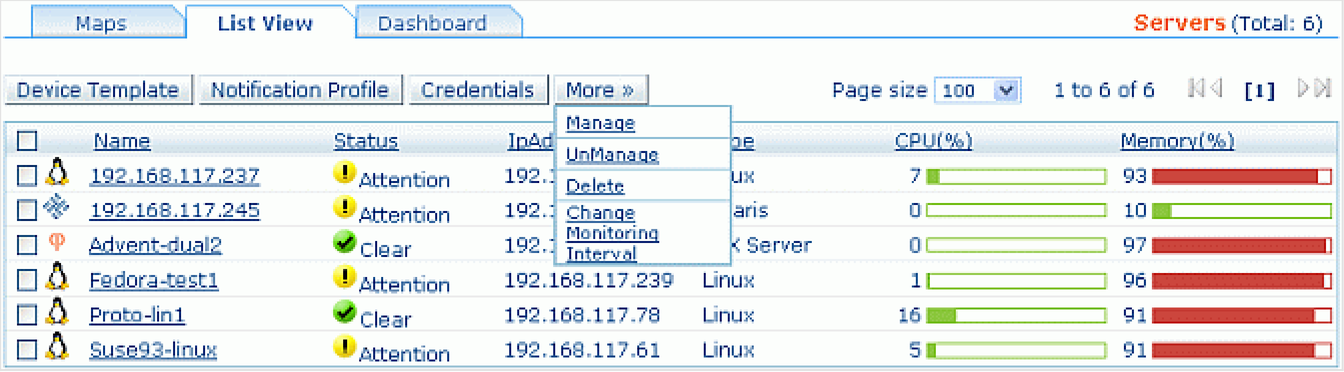
To delete a CCTV follow the steps given below:

1. Mouse over **Dashboards** and click **Manage CCTV.**
2. Click the trashcan icon that is corresponding to the name of the CCTV that you want to delete.
3. A confirmation window pops up.
4. Click **OK** to confirm deleting the CCTV.

The CCTV is deleted.

List View

The List view (Maps-> <Device Category>-> List View) lists all the devices of a category along with their Status, IP Address, Type, % of CPU utilized and % of memory utilized in order to have a quick look at the current status and workload handled by the devices.



□	Name	Status	IpAd	pe	CPU(%)	Memory(%)
□	192.168.117.237	Attention	192.1	ux	7	93
□	192.168.117.245	Attention	192.1	aris	0	10
□	Advent-dual2	Clear	192.1	Server	0	97
□	Fedora-test1	Attention	192.168.117.239	Linux	1	96
□	Proto-lin1	Clear	192.168.117.78	Linux	16	91
□	Suse93-linux	Attention	192.168.117.61	Linux	5	91

The following actions can also be done from here:

- Applying a Device Template
- Associating Notification Profiles
- Applying Credentials
- Managing/Unmanaging Devices
- Deleting Devices
- Changing the monitoring interval of the devices

Applying a Device Template

To apply a device template to the device templates, follow these steps:

1. Select the devices for which you want to apply the template.
2. Click on **Device Template** button.
3. Select the Device Template which you want to apply to the devices.
4. Click **Apply**.

The selected device template is applied to the selected devices.

Associating a Notification Profile

1. Select the devices.
2. Click on **Notification Profile** button.
3. Select the profile to be associated to the devices and click **Next**.
4. Select the fault criteria for the selected profile and click **Next**.
5. Select one of the following options to select the time-window:
   - Apply this profile all the time- This notifies alerts occurring for the selected criteria at any time.
   - Apply the profile for the selected time window- You can specify the required time- window here. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, alerts triggered during the specified interval and selected days only will be notified.
6. Click **Associate** button.

The notification profile gets associated to the selected devices. Note: The notification profiles that are already associated with the devices are left unchanged.

Applying Credentials

1. Select the devices to which you wan to apply the credentials.
2. Click on **Credential** button.
3. Select the credential that you want to get applied to the selected devices.
4. Click **Save**.

The selected credential gets applied to the selected devices.

Managing and Unmanaging devices

1. Select the devices that you want to move to managed or unmanaged state.
2. Click on **More** button and click **Manage**/**Unmanage**.

The selected devices gets changed to managed or unmanaged state accordingly.

Deleting devices

1. Select the devices that you want to delete or remove from OpManger.
2. Click on **More** button and click **Delete**.
3. A confirmation window pops-up.
4. Click **OK** to confirm deleting.

The selected devices are removed from OpManager.

Changing the Monitoring Interval

1. Select the devices whose monitoring interval has to be changed.
2. Click on **More** button and click **Change Monitoring Interval**.
3. Enter the required monitoring interval in terms of minutes.
4. Click **OK**.

The monitoring interval of the selected devices is changed.

Infrastructure Views

Mouse-over Maps tab to access Infrastructure views from the subtabs.

The various category of devices such Servers, Routers, Firewalls etc. monitored by OpManager are listed under Infrastructure Views.Clicking on the Category name, opens the Map View of that category. OpManager also provides you the option to create you own infrastructure view.

Google Maps

OpManager allows you to integrate Google Maps and place the devices on the maps according to the geographic distribution. Here are the steps to integrate Google Maps and Place devices on them.

- **Providing the Google Maps API Key**

1. Make sure you have a Google Account or create one.
2. Mouse-over the Maps tab in the OpManager WebClient.
3. Click on **Google Maps** link in the Business Views column.
4. You will be prompted to enter the key. Click on the link **Sign up for a Google Maps API key** to generate a key. You will be taken to a sign up page.
5. Scroll down the page and provide the website URL as http://<host name running OpManager>. For instance, if the name of the device running OpManager is OpM-Server, your URL will be http://OpM-Server.
6. Click on the **Generate API Key** button. A key is generated.
7. Copy the entire Key.

- **Viewing the Google Map in OpManager WebClient**

1. Go back to the OpManager Webclient and provided the key in the corresponding field.
2. Click on **Submit Key**.
3. The Google Map is shown in the interface.

- **Adding Devices on the Google Map**

1. Now, zoom in/out the map and double-click on the location where you want to place a discovered device.
2. A device list box pops up allowing you to select a device to be placed in that location.
3. Select the device and click on **Add**.
4. Add the required devices on to the map by double-clicking the location.
5. You can also add the devices to the map from the device snapshot page.
6. Go to the device snapshot page.
7. Click on **Add to Google Map** link in the page to add the device to the map.

- **Viewing Device Details from Google Map**

1. Click on the device balloons on the Google Map to see a popup.
2. Click the device name/ip address on this popup to get into the device snapshot page.
3. The popup also shows the device status.

- **Deleting Devices from Google Map**

1. Click on the device balloons on the Google Map to see a popup.
2. Click the **Delete** link on this popup to delete the device from the map.

Business Views

OpManager (from build 7000 onwards) comes with an in-built flash-based MapMaker. No more hassles of invoking a separate tool to create business views.

- Adding Business Views
- Drawing Link between Devices
- Modifying Business Views
- Adding Shortcuts

Click the small down arrow in the Maps tab or simply mouse-over. The default maps, with options to add more maps are seen.

Adding Views:

1. From the pop-up in the Maps tab, click Add Business View option.
2. Configure a name for the business view.
3. From the available devices list, select the devices you want to be grouped in this business view, and move them to the right-to the Selected Devices column,
4. Select the background from the corresponding list box.
5. Click Apply.
6. Drop the devices on the map and click on the confirmation check-box that appears.
7. Once the devices are dropped on the map, select and drag-drop the devices to be placed in the required location on the map.
8. Click **Save** button on the left to create and save the map.
9. Click **Exit** to see the newly created business view. You will also find the availability dashboard for the devices in the business view.

Drawing a Link Between Devices

To represent the network diagram in the map, OpManager allows you to draw links between the devices in a business view. You can assign a meaningful name to the link and also configure to change the color of the link to indicate its status.

To draw a link, follow the steps given below:

1. Click the **Add Link** button on the left.
2. From the map on the right, click the device from which you want to draw a link (the source device) and move the mouse to the destination device and click that device. A link properties dialog pops up.
3. Configure a display name for the link.
4. In the **Get Status from** field, select any interface from either the source device or the destination device. The link will inherit the status of the interface that you choose here. For instance, if the source device goes down, and if you have selected an interface from that device, the link also inherits the status of that device.
5. Select the line type and size.
6. Deselect the **Show Arrow** check box if you don't want to show the traffic arrows.
7. Click **Apply**.
8. Click **Save** on the left to save the changes.

Modifying Business Views

You can make changes to the business views created. Access the business view either from the Maps tab or from the list of views under the Home tab. Click the Edit icon to modify the view properties. After you modify the properties like adding/removing links, adding more devices to the view, adding shortcuts on the view, changing background etc, click the **Save** button on the left to save the changes.

Adding Shortcuts

You can add shortcut icons to business views that helps you to drill-down the network. This helps you to easily navigate to a view from another view when objects are grouped based on their geographical location.

Note: You must have created atleast two business views to be able to add a shortcut from one view to another.

Here are the steps to add shortcuts on the business views:

1. Go the the business view and click the Edit option on right-top corner of the view.
2. Click the Add Shortcut button on the left. A shortcut properties dialog pops up.
3. Configure a name for the shortcut in the **Shortcut Name** field.
4. From the **Open Submap** list-box, select the map which should be opened when you click the shortcut.
5. Select the icon to be used for the shortcut from the **Default Icons** or select from the **Custom Icon** combo-box.
6. Click Apply for the shortcut to be added.

Network Views

Mouse-over Maps tab to access the network views. The various networks that are discovered and monitored by OpManager are listed under Network Views. Clicking on the network's IP address opens the Map view of that network. Clicking on Network Map link displays the layout of that network's LAN connection.

Managing Faults in Network

There can various types of faults in a network. With the network health depending on various resources like the system resources, services, network connectivity etc, getting to the root of the problem is simplified when the monitoring solution raises meaningful alarms. OpManager helps you identify the fault quickly with its detailed alarms indicating the resource that is poorly performing in the device . The different types of OpManager alarms include:

- Status-poll Alarms (device, service, interface, port down alarms).
- Threshold-based alarms for host resources, response times etc proactive monitoring.
- Alarms from SNMP Traps.
- Windows event logs based alarms.

OpManager monitors the resources for availability and performance and triggers alarms for all the criteria mentioned above. These alarms can also be sent as email or sms alerts from OpManager.

Viewing Alerts

The Alarms tab in OpManager shows all the latest alerts.

From the list box on the top right corner, you can access the following:

- **All Alarms**: A complete list of alarms is displayed here.
- **Active Alarms**: This view lists only the active alarms that are not yet cleared.
- **Unsolicited Traps**: The unsolicited traps sent by the agents in the managed devices are listed here. These are the traps that are not configured to be processed in OpManager. If you find any of these traps to be critical, you can configure OpManager to process the traps using the information received from the agent. Refer to Creating a Trap Processor for details.
- **Windows Events**: This view lists only the alarms that are triggered from Windows event logs as the source.
- **Devices to Watch**: You can view the devices with fault in this list view.
- **Syslog Alarms**: This view lists only the alarms logged via syslog.

Alert Actions

You can perform the following alert actions:

Acknowledge: This option is useful for the operators to pick up the problem and work on it. When you select an alarm and click on Acknowledge button on top the alarms list, the administrator/operator's name is populated in the technician's field. Note: Alarms that are acknowledged can be excluded from being escalated by configuring accordingly the alarm escalation rule.

Unacknowledge: The assigned technician is removed and the alarm is back in the unassigned list.

Clear: You can click this to clear an alarm manually.

Delete: You can delete an alarm.

View History: Click on the alarm message to view the alarm details and event history.

Add Notes:You can add notes to the alarms to explain the steps you have followed to correct the fault or to give tips to the operator who is working on the fault. In the Alarm history page, click the **Add Notes** option.

Execute Workflow: You can execute a workflow to troubleshoot an alarm. Click on **Execute Workflow** in the Alarm Details page, and select the workflow. The workflow will be executed and the output will be added in the notes.

Test Actions: You can notify this alarm via any of the notification profiles created by you. Click on **Test Actions** in the Alarm Details page, and select the desired notification profile.

View Availability: You can view the availability history of the faulty device. Click on **More** link in Alarm Details page and select **Availability**.

Ping: You can ping the faulty device. Click on **More** link in Alarm Details page and select **Ping**.

Trace Route: You can trace route the faulty device. Click on **More** link in Alarm Details page and select **Trace Route**.

Unmanage: Alarms created for devices that are under maintenance can be can be avoided by moving the device to unmanaged state. Click on **More** link in Alarm Details page and select **Unmanage**.

Configure Notifications: You can configure a notification profile to the faulty devices. Click on **More** link in Alarm Details page and select **Configure Notifications**.

Escalating Alarms

The alarms of critical devices should not be left unnoticed for a long time. For instance, the mail-servers, web-servers, backup-servers, switches, and routers are so critical that if their faults are not solved within a specified time, the networking functionality will be brought down. You can configure OpManager to escalate such unnoticed alarms by sending an e-mail to the person concerned. However, you have an option to exclude the alarms that are acknowledged from being escalated.

To configure a new alarm escalation rule, follow the steps given below:

1. Click the **Admin** Tab.
2. Under **Alerts**, click **Alarm Escalation**.
3. Click **Add Rule** to create a rule.
4. Assign a name to the rule in the **Rule Name** field.
5. Select the **Severity** and **Category** of the alarm.
6. Select the **Business View** in order to associate the rule only to the alarms of the devices of the selected business view. If not select None to associate the rule to the alarms of all the devices.
7. Then configure the the interval in either hours or minutes to wait for the alarm to get cleared.
8. You can exclude the acknowledged alarms from being escalated by selecting **Exclude Acknowledged Alarms** option.
9. Type the values for the fields under **Escalation Email Details** to send an e-mail if the alarm is not cleared within the specified interval.
10. Configure the **From Email Address**, the **Subject** and the **Message** of the escalation mail.
11. In the **Run this check every** box, set the interval in minutes to execute this rule.
12. Click **Save**.

If you configure a new alarm escalation rule, by default it will be enabled. To disable an alarm escalation rule click on Edit icon, deselect the **Enable this rule** option and click on **Save**.

Alarm Suppression

OpManager provides you the option to suppress the alarms of the devices for a pre-defined time interval. This option will be very useful in cases, where the devices are under maintenance or some known issues exist with them.

Configuring Alarm Suppression for a Single Device

1. Go to the device snapshot page.
2. Click on Actions tab and select Suppress Alarms.
3. Select the period for which you want to suppress the alarm.
4. Click Close Window.

Alarms of this device will be suppressed for the selected period

Configuring Alarm Suppression for Multiple Devices

1. Under Admin tab click Quick Configuration Wizard.
2. Select the option Associate an Alarm Suppression rule to several devices and click Next.
3. Select the time period for which you want to suppress the alarms.
4. Select the Category of the devices for which you want to associate or manually group the devices.
5. Click Next/Finish accordingly.

Receiving SNMP Traps in OpManager

OpManager listens for SNMP traps from devices on the default port 162. So, it automatically acts as a trap receiver and based on the trap processors defined in OpManager, the traps are processed and shown as OpManager alarms.

Processing SNMP Traps into Alarms

What is SNMP Trap?

Traps are cryptic messages of a fault that occurs in an SNMP device. SNMP traps are alerts generated by agents on a managed device. These traps generate 5 types of data:

- Coldstart or Warmstart: The agent reinitialized its configuration tables.
- Linkup or Linkdown: A network interface card (NIC) on the agent either fails or reinitializes.
- Authentication fails: This happens when an SNMP agent gets a request from an unrecognized community name.
- egpNeighborloss: Agent cannot communicate with its EGP (Exterior Gateway Protocol) peer.
- Enterprise specific: Vendor specific error conditions and error codes.

Processing SNMP Traps into Alarms

OpManager enables you to process the traps from the managed devices.

- When a trap is received from a managed device, the match criteria in the parser determines whether a specific trap matches the conditions specified in the Trap Processor. Once a matching Trap is found, an alert is generated.
- Trap Processor Converts the cryptic message to human-readable alarm.
- Configure OpManager to process the traps that are not processed out-of-the-box and convert them into alarms.
- The traps that are not processed are listed under 'Unsolicited Traps'.

Tools

The following actions can be done by clicking the relevant icon:

- Edit: Edit the Trap
- Enable or disable trap processing: Click to enable/disable trap processing
- Delete processor: Delete the Trap Processor
- Search Processor: Enter the start or end letters of the trap name to search for a trap. You can search by entering an OID too.

Adding/Modifying Trap Processor

1. Go to **Admin** --> **SNMP Trap Processors**.
2. Click ‘**Add New Trap**’ to process the unsolicited traps.
3. Click the **TrapParser** name/ Edit icon to modify an existing one.
4. Configure/Modify the following properties:

- **Trap Name**: Configure a name for the new trap processor.
- **Description**: Describe the trap.
- **Snmp Trap Version**: Select the version (SNMP V1/V2c).
- **SNMP V1 Properties**:
  - Generic Type: Cold Start, Link Up, Enterprise, etc. Select the appropriate type for the OID
  - Specific Type: When Generic Type is set to Enterprise a specific trap ID s identified
  - Enterprise OID: Corporation or organization from where the trap originated, such as .1.3.6.1.4.1.x SNMP V2C / V3
- **SNMP V2 Properties**:
  - Trap OID: For devices with SNMP v2c version, select the trap oid from the MIB using the Select button.
- **Message**: Select the required message variables.
- **Severity**: Select the Alarm severity.

- Advanced: Click this button to specify the following match conditions for finer processing of traps.
  - Match Criteria: Select the appropriate radio button to either match any one or all the conditions that you specify. Select the variable bindings, the condition, and the string to be matched.
  - Rearm Criteria: Similarly, select the appropriate radio button to match the rearm conditions. Select the variable bindings, the condition, and the string to be matched.
  - Failure Component: This option is useful when you deal with a single trap OID that has multiple failure components. The Varbinds containing more details on the trap will have information on the failed components (entities like cpu, temperature etc). You can match the entity too by appending the VarBind number in this field to generate separate alarms for the failed components. For instance, $Source_trapName_trap_$v5.
  - Source: Append the Varbinds to be matched if required. This option is useful if the trap is forwarded from another source.
- Click **Add**/**Save** for the configuration to take effect.

Loading Trap Parsers from a MIB

Following are the steps to load the traps from various MIBs

1. Under the **Admin** tab, select **SNMP Trap Processors**. All the configured processors are listed here.
2. On the right, click on **Load Traps From Mibs**.
3. From the list of MIBs, select the MIB from which you would like to load the trap variable. The traps in that MIB are listed.
4. Select the required trap variable, and click **Add Trap Processor(s)**.

A Processor for the selected trap is added, and is listed under the SNMP Trap Processors.

How to process the Unsolicited Traps?

1. Click on **Unsolicited Traps** in Alarms tab.
2. Click on **Create Trap Processor** corresponding to the trap message.
3. Type a name for **TrapName**.
4. Make sure that the status is enabled.
5. Select the **Severity**.
6. Click on **Add**.

How to configure SNMP Traps in Agent ?

Despite configuring the SNMP Trap Processor in opmanager, you might still not see the alarms based on traps. You might need to check the SNMP agent configuration on the monitored devices.

Configuring Notifications

When a fault is detected in your network, an event occurs and multiple events correlate to trigger an alarm. You can configure OpManager to notify the network administrator or perform automatic actions based on the alarm raised for a device.

The different types of notifications available are:

- Email Alerts
- SMS Alerts
- Web Alerts
- Run a Program
- Run a System Command
- Log a Ticket (Trouble ticketing in ServiceDesk Plus)

The configured notification settings are available as profiles and these can be associated to different devices for different fault criteria.

Configuring Mail Server Settings

OpManager allows you to configure e-mail alerts and SMS alerts to get notified on the fault in your network. By default, OpManager sends the mail to the mail server specified in the e-mail notification profile. To configure the SMTP server settings globally and to provide the secondary mail server settings, follow the steps given below:

1. Under the **Admin** tab, click **Mail Server Settings**.
2. Enter the SMTP **Server name** and **Port** number.
3. Configure the **From** and **To Email ID** fields.
4. Enter a **Time Out** interval.
5. Configure the **User name** and **Password** details, if the server requires authentication to send e-mail.
6. For SSL authentication, select the **SSL Enabled** check-box, browse and select the SSL certificate and key-in the password.

Verifying Configuration

- To test the settings enter the **Email ID** and click **Test Mail**. This e-mail ID will be considered as the default To Email ID while creating Email and SMS notification profiles.
- If you have a secondary mail server in your network, select **Add a secondary mail server** and provide the details. In case of failure of primary mail server, OpManager uses secondary mail server to send e-mail and SMS.

Configuring Proxy Server Settings

Any business enterprise will have a proxy server to optimize its connectivity to Internet and to filter access to restricted Web sites. In OpManager, to monitor URLs over internet, you need to provide the proxy server details of your enterprise.
To enter the details, follow the steps given below:

1. Under the **Admin** tab, click **Proxy Server Settings**.
2. Select the **Enable Proxy** check-box.
3. Enter the Proxy server name, port number in which the Web service is running on the proxy server, and the user name and password to connect to the proxy server.
4. For the devices that do no require to go through a proxy, specify the name or the IP Address of the devices as a comma separated list in the **No Proxy** field.
5. Click **Save** to save the details.

Configuring SMS Server Settings

Besides the email-based SMS notifications, OpManager allows you to configure modem-based SMS alerts. Configure the SMS Server Settings in OpManager as follows:

1. Ensure if yours is one of the supported modems.
2. Connect the GSM Modem to the Serial Communication Port.
3. Go to Admin --> SMS Server Settings.
4. Configure the port number to which the Modem is connected.
5. Click OK.

Forwarding Syslog

You can forward the syslog received in OpManager to any NMS.

Steps to forward syslog:

1. Go to **Admin**-> **Syslog Rules**.
2. Mouseover **Actions** and select **Forward Syslog**.
3. Click on **Add Destination** button.
4. Provide the name/IP address of the NMS Host to which SysLog has to be forwarded.
5. Provide the SysLog listening port number of the NMS to which SysLog has to be forwarded.
6. Click on **Start Forwarder** to initiate sending of SysLog to the destination NMS. You can also **Stop Forwarder** at any desired time.

Forwarding Traps

Configure OpManager to notify users over a Trap when there is a specific fault.
Steps to forward Traps:

1. Configure a **name** for the notification profile.
2. Provide the **name/IP address** of the host to which notifications has to be sent.
3. Provide the trap listening **port** number of the host to which notifications has to be sent.
4. Select the trap **version**, either v1 or v2c.
5. Provide the **community** string for the trap(defaults to public).
6. Select the trap variables that should appear in the notifications. To receive the traps, relevant OPMANAGER-MIB should be downloaded and made available in receiving host. You can find this MIB under the folder location (OpManger -> mibs)
7. Click **Save** to create the profile.

You have successfully configured the notification profile.

Configuring Email Alerts

You can configure OpManager to send e-mail to network administrators when a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever the device has a fault, an e-mail is sent to the technician concerned.

To create an email alert profile, follow the steps given below:

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Email Alerts**.
3. Type the profile name.
4. Type valid **To** and **From** Email addresses.
5. Select the required alarm variables that you would like to see in the email alert.
6. Click Associate link on the right to associate the profile to devices.
7. Select the Profile and click **Next**.
8. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next
9. Select the devices or the category of devices for which you want to be notified. For instance, if you want to be notified of threshold violation for all Servers, select Server category from the combo-box. Click Next.

The profile is associated to all the servers. A notification is sent every time a threshold is violated for a server.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new email profile is created, the values of the primary SMTP server and the authentication details are retrieved from the Mail Server settings. Refer to Configuring Mail Server Settings for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server is used to send the mail automatically.

Configuring SMS Alerts

You can configure OpManager to send SMS to network administrators whenever a fault is detected in the device. You can create separate profiles for each administrator and assign them to devices so that whenever a device has trouble, depending on the trouble, SMS is sent to the technician concerned.
OpManager supports email-based SMS alerts and also modem-based SMS alerts.
Please note that Modem-based SMS alerts comes as an add-on over OpManager and needs to be licensed seperately.

Modem-based SMS Alerts

To create a modem-based SMS notification profile, here are the steps:

1. Configure the SMS Server Settings.
2. Click the **Admin** tab.
3. Under **Alerts**, click **Notification Profiles**.
4. From **Modem-based SMS** column, click **Add New**.
5. Type the profile name.
6. Type the mobile number.
7. Select the required alarm variables. The selected variables will be seen in the sms alert received.

Refer to the support modems list to use this notification profile.

Email-based SMS Alerts

To create an email-based SMS notification profile, follow the steps given below:

1. Configure the Mail Server Settings if you have'nt configured yet.
2. Click the **Admin** tab.
3. Under **Alerts**, click **Notification Profiles**.
4. From **Email-based SMS** column, click **Add New**.
5. Assign a meaningful name to this profile.
6. Type valid To and From Email addresses.
7. Select the required alarm variables that you would like to see in the sms alert.
8. Save the Profile.
9. Associate the profile to the required devices. This triggers alerts when faults occur.

Note: Primary and secondary SMTP server settings can be provided in the Mail Server Settings page in OpManager. Whenever a new SMS profile is created, the values of the primary SMTP server and the authentication details will be considered from the Mail Server settings. Refer to Configuring Mail Server Settings for steps to enter the details. If the SMTP server is not available while sending e-mail, secondary mail server will be used to send the mail automatically.

Configuring Web Alarm Notifications

Configure OpManager to notify you by way of a web alarm when there is a specific fault.

Here are the steps to configure a Web Alarm Notification Profile:

1. Go to Admin > Notification Profiles > Web Alarm
2. Click **Add New** against the Web Alarm profile.
3. Configure the following values to create the profile:
    - **Profile Name**: Configure a name for the notification profile.
    - **Select Users**: Select the users for whom Web Alarms should be enabled.
    - **Test Actions**: Click this button to confirm if the Web Alarm sound is produced.
4. Click **Save** to create the profile.

You will hear the alarm sound when logged-in as any of the selected users.

Note: The Web Alarms are available only for the user sessions selected above.

Using a Run Program Notification Profile

You can configure OpManager to automatically run a program whenever a fault is detected in the device. For instance, you can configure OpManager to execute a program that corrects the fault or simply produces a sound or that whenever a specific type of an alarm is raised for a device.

To create a profile that executes the specified program, follow the steps given below:

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Run Program**.
3. Type the profile name.
4. In the **Command Name** field, specify the name of the program to be executed with the absolute path. Example C:profilestestprogram.bat.
5. If the program requires some arguments, specify the arguments.
6. Save the profile.
7. Click Associate link on the right to associate the profile to devices.
8. Select the Profile and click Next.
9. Select the fault criteria for which you need to be notified. For instance, if you want to be notified of threshold violation, select 'Threshold rule is violated'. Click Next
10. Select the devices or the category of devices for which you want to be notified. Click Next.

The profile is associated to all the servers. The program is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Logging a Trouble Ticket to ServiceDesk Plus

Following are the steps to configure a notification profile to log a trouble ticket to ServiceDesk Plus.

1. Ensure that the servers settings are configured properly.
2. Under Admin tab, click Notification Profiles.
3. On the right, click **Log a Ticket** under **Add New**
4. Configure the following notification profile details
   - Profile Name
   - Choose the appropriate device category from the **Category** combo-box
   - Choose the priority of the issue from the **Priority** combo-box
   - Choose a technician to whom the issue is to be assigned from the **Technician** combo-box
   - Select the alarm variables such as the alarm severity, device display name etc, from the corresponding combo-box under **Ticket Contents**. These details are displayed on the issue title.
   - Select the required alarm variables to be included for the alarm description. This will provide accurate fault information to the assigned technician
   - Click **Submit**.

After the profile is created, you can associate it to the required devices.

Using a Run Command Notification Profile

You can configure OpManager to automatically run a system command whenever a fault is detected in the device. For instance, you can configure OpManager to execute a netsend command to send popup messages to users machines whenever a specific type of an alarm is raised for a device.
To create a profile that executes the specified program, follow the steps given below :

1. Select Admin --> Notification Profiles
2. Click **Add New** option against **Run System Command**.
3. Type the profile name.
4. In the **Command String** field, specify the command name with additional arguments if any.
5. Select the **Err Append** and **Append** check-boxes to append the output and the error message on executing the command.
6. Save the profile.
7. Associate the profile to devices.

The system command is executed with the specified arguments whenever a fault matching the selected criteria occurs.

Notifications via Traps

Configure OpManager to notify users over a Trap when there is a specific fault.

Steps to configure a trap profile:

1. Go to **Admin**-> **Notification Profile**.
2. Click on the **Add New** link in the **Trap Profile** widget.
3. Configure a **name** for the notification profile.
4. Provide the **name/IP address** of the host to which notifications has to be sent.
5. Provide the trap listening **port** number of the host to which notifications has to be sent.
6. Select the trap **version**, either v1 or v2c.
7. Provide the **community** string for the trap(defaults to public).
8. Select the trap variables that should appear in the notifications. To receive the traps, relevant OPMANAGER-MIB should be downloaded and made available in receiving host. You can find this MIB under the folder location (OpManger -> mibs)
9. Click **Save** to create the profile.

You have successfully configured the notification profile.

SysLog Notification Profile

When any fault occurs you can notify users via SysLog.

Steps to configure a SysLog profile:

You can choose any of SysLog severity events to be processed.
Note : $severityrefers to alarm severity in OpManager. These alarm severities will be automatically parsed and inter-mapped with SysLog severities before being sent as a SysLog notification. The below table will explain you the mapping between OpManager and Syslog severities.

OpManager Severity	**SysLog Severity**
Critical	Critical
Trouble	Error
Attention	Warning
Service Down	Warning
Clear	Informational

1. **Admin**-> **Notification Profile**.
2. **Add New** link in the **SysLog Profile** widget.
3. **name** for the notification profile.
4. **name/IP address** of the host to which notifications has to be sent.
5. **port** number of the host to which notifications has to be sent.
6.
7.
8. **Save** to create the profile.

You have successfully configured the notification profile.

Creating a Sound Notification Profile

By default, OpManager provides a sound notification that plays a beep sound when a fault is detected in the associated devices. You can also create profiles to play the sound of your interest.
To create a sound profile, follow the steps given below:

1. Copy the sound file you want to play in the *<OpManager Home>/conf/application/scripts* directory.
2. Create a Run Program notification profile with the following values to the fields:

   Command Name: ./jre1.4.1/bin/java

   Program arguments: -classpath ./classes/OpManagerServerClasses.jar com.adventnet.me.opmanager.server.alert.AudioNotifier ./conf/application/scripts/<audio_file_name>

You need to associate the profile to the device for triggering it during a fault. The sound can be heard in the OpManager server.
.

Modifying and Deleting Notification Profiles

You can modify or remove an existing notification profile. Here are the steps:

1. From the Admin tab, select **Notification Profiles**.
2. All the configured profiles are listed here.
3. Click the **Delete** icon against the profiles name to delete the profiles.
4. Click the **Edit** icon against the profiles name to modify the profile properties.

The changes made here are applied for all the devices to which the profile is associated.

Associating Notification with Managed Devices

You need to associate the notification profiles with devices to trigger the corresponding action whenever these devices are under trouble. You can also select the time-window so that alerts during the specified interval only is notified.
To associate a profile with devices or a category of devices, you can use the Quick Configuration wizard. For doing so, follow the steps given below:

1. From the **Admin** tab, under **Configuration**, click **Quick Configuration wizard**.
2. Select **Assign a notification profile...** and click **Next**.
3. Select the profile to be associated to the devices and click **Next**.
4. Select the fault criteria for the selected profile and click **Next**.
5. Time Window: Select one of the following options:
   - Apply this profile all the time- This notifies alerts occurring for the selected criteria at any time.
   - Apply the profile for the selected time window- You can specify the required time- window here. For instance, if you set the values as From 09:30 To 18:30, and select the days from Monday through Friday, alerts triggered during the specified interval and selected days only will be notified.
6. Delayed Trigger: If you want the notification profile to be triggered at a delay, enter the delay time (in minutes). If you don't want to trigger the notification profile if the alarm has been acknowledged in the mean time, you can select the 'Do not trigger if alarm is acknowledged' check box.
7. Recurring Trigger: This option helps you trigger the notification profile at regular intervals, till the alarm is cleared. Enter the trigger interval and number of triggers. If you don't want to trigger the notification profile repeatedly if the alarm has been acknowledged, you can select the 'Do not trigger if alarm is acknowledged' check box.
8. Click **Next**.
9. Select one of these options to associate the profile and click **Next**.
   - If you select a category, then the profile is associated to all the devices in the category automatically.
   - If you choose Select devices manually, the next page will list all the managed devices. Move the devices from the list in the left to the one in the right and click **Finish**.
   - If you select a business view, the profile is associated to all the devices in the selected view.

To associate a notification profile to a single device, follow the steps given below:

1. Open the snapshot page of the device.
2. Select the **Notification Profiles** tab at the bottom.
3. Click the corresponding link to select and associate the required profiles.

Monitoring VMware ESX/ESXi servers

OpManager monitors your VMware servers for availability and performance using native APIs. The advantage of using native APIs is that it does not require any agent to be installed on your servers. Moreover, it enhances the usability and offers in-depth monitoring capabilities to troubleshoot your Virtual Infrastructure.

Some of the highlights of monitoring VMware Servers with OpManager:

- Supports ESX/ESXi 3.5 to latest version 5.1
- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Supports monitoring of hardware health such as temperate, voltage, power, fan speed, status of processors, disk arrays, etc. of HP, Dell and Cisco systems, via SNMP.
- Out-of-the-box 70 plus reports on Host and VMs
- Automatically maps the VMotioned VMs to the corresponding Hosts

Apart from monitoring the Hosts and VMs, OpManager also monitors the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP.

Pre-requisites for monitoring VMware ESX/ESXi Servers

- HTTPS User Name and Password: As OpManager uses native APIs to monitor the VMware servers, it requires https username and password of the Host server to poll the performance data. Provide the correct https username and password when discovering the Host.
- VMware Tools (optional): We recommend that you install VMware tools on the VMs. In general, VMware tools improve the performance of the Virtual Machine. Moreover, they offer IP address of the VMs, which helps OpManager to automatically discover them. Click here to know the procedures for installing VMware tools.

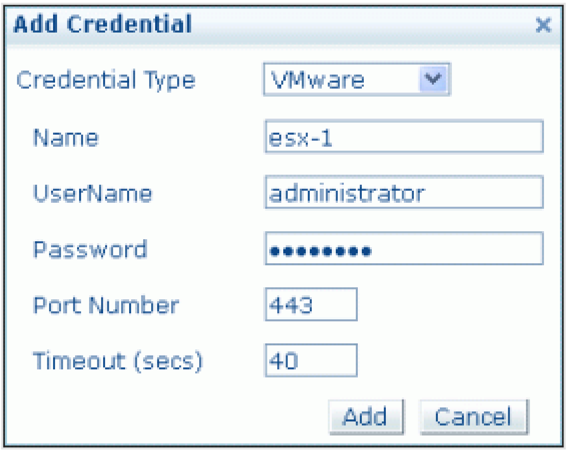
Discovering VMware ESX/ ESXi servers in OpManager

To discover the host and the VMs, you just need to provide the IP Address and https credentials of the vCenter/ Host. When you provide the vCenter credentials, all the host and VMs managed by that particular vCenter will be discovered. In-case of providing the Host credentials, the host along with its VMs are discovered.

Steps to discover the Host and VMs

Before proceeding ensure that you have configured the VMware credentials for the vCenter/ Host, and SNMP and WMI credentials for the VMs in the Credential Library. To configure the credentials

1. Go to **Admin**-> **Credential Settings** and click **New** button.



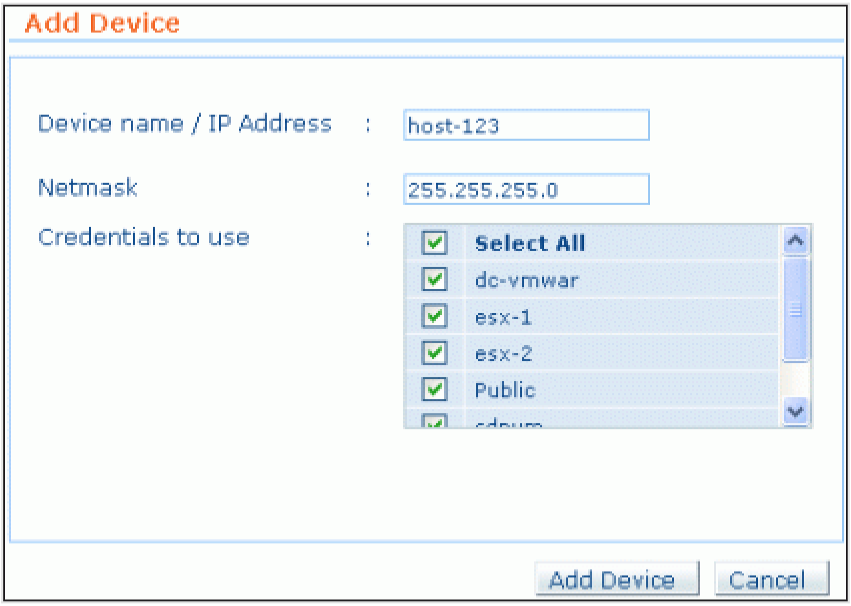
Credential Type	VMware
Name	esx-1
UserName	administrator
Password	••••••••
Port Number	443
Timeout (secs)	40

2. Select VMware as the **Credential type** and enter the vCenter/ Host Name and its HTTPS **Username** and **Password**.
3. Enter the HTTPS web service **port number** and **timeout** interval for the connection between the vCenter/ Host and OpManager server.
4. Click **Add** to add the credential.

Similarly, add the credentials for the VMs. Select the Credential Type as WMI for Windows and SNMP for non-Windows OS.

To discover the vCenter/ Host:

1. Go to **Admin**-> **Add Device**. (You can also access the Add Device window from **Maps**-> **Virtual Devices**-> **Add New vCenter/ Host**).
2. Enter the **Device Name / IP Address.**



Add Device

Device name / IP Address	:	host-123
Netmask	:	255.255.255.0
Credentials to use	:	☑ Select All ☑ dc-vmwar ☑ esx-1 ☑ esx-2 ☑ Public ☑ sdpvm

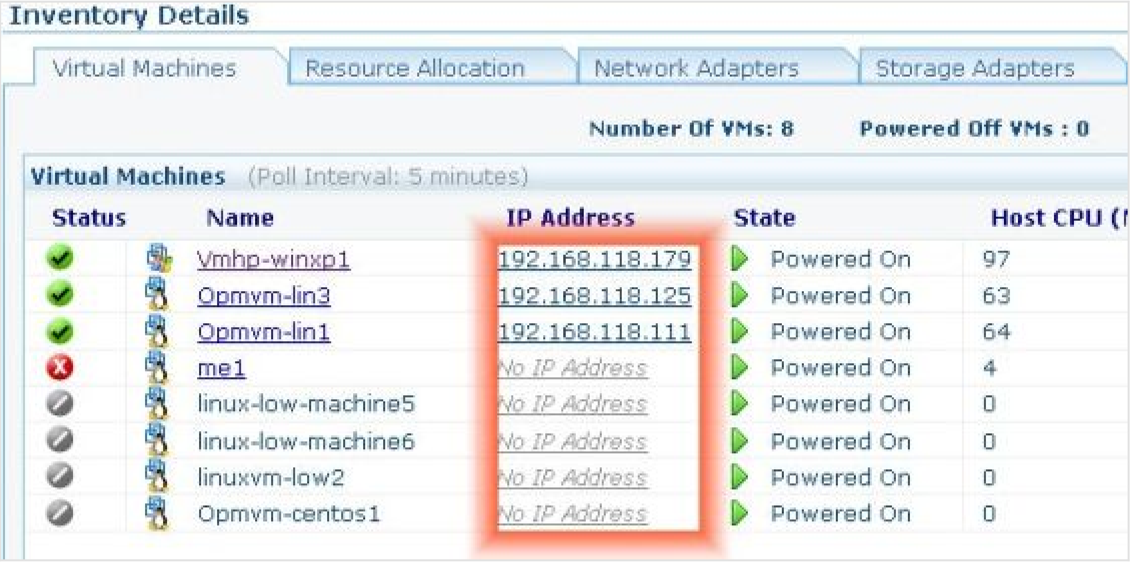
3. Enter the correct **Netmask** and select the appropriate **credentials**.
4. Click **Add Device** button to add the vCenter/ host.

If any of the VMs are already discovered or added, OpManager automatically maps them as Virtual Device. Once the discovery is over you can find the Host & VMs under 'Virtual Device' category in Maps tab.

Note: If the device has been added successfully, but not displayed under the Virtual Devices map, search for that device. Go to its snapshot page and look for the device type. If it is mentioned as ‘unknown’, wrong credentials might have been provided or it is not reachable during discovery. Provide the correct credentials and click on ‘Rediscover Now’ under Actions tab in the snapshot page, to discover it as an ESX host.

Configuring VM IP Address

OpManager, with the help of installed VMware Tools, identifies the IP address of the VM and maps it to the host. In case the VMware Tools are not installed, OpManager discovers it using VM's entity name. You can assign the IP address for such VMs in the host snapshot page (screenshot of the same is given below). Click on the 'No IP Address' link corresponding to the VM to assign the IP address for that VM. Similarly, you can click the assigned IP address to choose another one as the primary IP for that particular VM.



Inventory Details

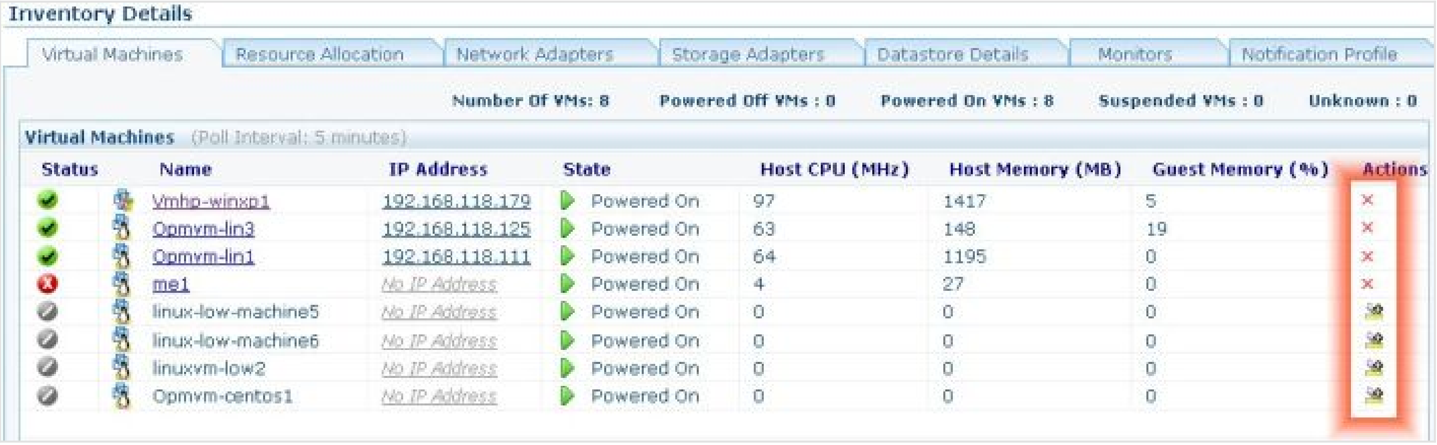
Number Of VMs: 8 Powered Off VMs : 0

Virtual Machines (Poll Interval: 5 minutes)

Status	Name	IP Address	State	Host CPU (
✓	Vmhp-winxp1	192.168.118.179	▶ Powered On	97
✓	Opmvm-lin3	192.168.118.125	▶ Powered On	63
✓	Opmvm-lin1	192.168.118.111	▶ Powered On	64
✗	me1	No IP Address	▶ Powered On	4
●	linux-low-machine5	No IP Address	▶ Powered On	0
●	linux-low-machine6	No IP Address	▶ Powered On	0
●	linuxvm-low2	No IP Address	▶ Powered On	0
●	Opmvm-centos1	No IP Address	▶ Powered On	0

Manage or Unmanage VMs

You can now choose to monitor only the required VMs on a Host. OpManager discovers all the VMs during the initial discovery and you will find them listed under the inventory in the host snapshot page. Click on the relevant icon to monitor the required VMs on the host. OpManager maintains this configuration when a HA, VMotion, or rediscovery happens.



Inventory Details

Number Of VMs: 8 Powered Off VMs : 0 Powered On VMs : 8 Suspended VMs : 0 Unknown : 0

Virtual Machines (Poll Interval: 5 minutes)

Status	Name	IP Address	State	Host CPU (MHz)	Host Memory (MB)	Guest Memory (%)	Actions
✓	Vmhp-winxp1	192.168.118.179	▶ Powered On	97	1417	5	✕
✓	Opmvm-lin3	192.168.118.125	▶ Powered On	63	148	19	✕
✓	Opmvm-lin1	192.168.118.111	▶ Powered On	64	1195	0	✕
✗	me1	No IP Address	▶ Powered On	4	27	0	✕
●	linux-low-machine5	No IP Address	▶ Powered On	0	0	0	
●	linux-low-machine6	No IP Address	▶ Powered On	0	0	0	
●	linuxvm-low2	No IP Address	▶ Powered On	0	0	0	
●	Opmvm-centos1	No IP Address	▶ Powered On	0	0	0	

Monitoring VMware ESX servers

All the discovered hosts and VMs are mapped under 'Virtualization' tab. Click on **Virtualization Devices** links to access the dashboard page, which provides a quick glance of your critical resources such as CPU, Memory, Network & Disk that are under pressure. Though ideal resource utilization is the key benefit we get from virtualization, it can lead to other problems because it is shared among the servers. Even if a single system has a resource crunch, it hugely affects the performance of the other systems running on the same host. Quickly identifying and fixing the resource utilization problems is therefore vital for a business to run smooth.

OpManager shows the top hosts and VMs by resource utilization and the recent alarms raised. Click on the host or the VM name to see its snapshot page. The Virtual Devices Dashboard page refreshes automatically every 5 minutes to reflect the latest collected statistics.

Listed below are the various types of top resource utilization widgets to quickly identify any over utilized resource. It gives a quick glance on systems which are the top consumers of CPU, Memory, Network, Disk I/O and Disk Space.

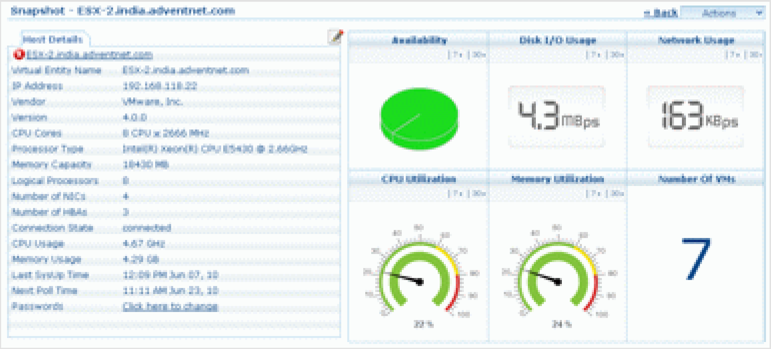
Top VMs	Top Hosts
1. Top CPU Consumers 2. Top CPU Ready Consumers 3. Top Memory Consumers 4. Top Swap Memory Consumers 5. Top Disk I/O Consumers 6. Top Network Consumers	1. Top CPU Consumers 2. Top Memory Consumers 3. Top Swap Memory Consumers 4. Top Network Consumers 5. Top Disk I/O Consumers 6. Top Disk Space Consumers

Snapshot page of a Host

Snapshot page of Host / VM provides a summary of the current statistics, recent alarms, configuration details such as VMs inventory, resource allocation for each VM, Network Adapters, HBA list and Datastores.

Host Details and Performance Charts

In this section you can find the Host details like IP Address, Vendor of Host, CPU Cores etc. on the left side. The right side gives a quick glance on performance data like CPU Utilization, Memory Utilization, Disk I/O Usage etc., collected during the last poll. These values are collected at an interval of 5 minutes. These data help you determine the current performance of the Host.



Snapshot - ESX-2.india.adventnet.com

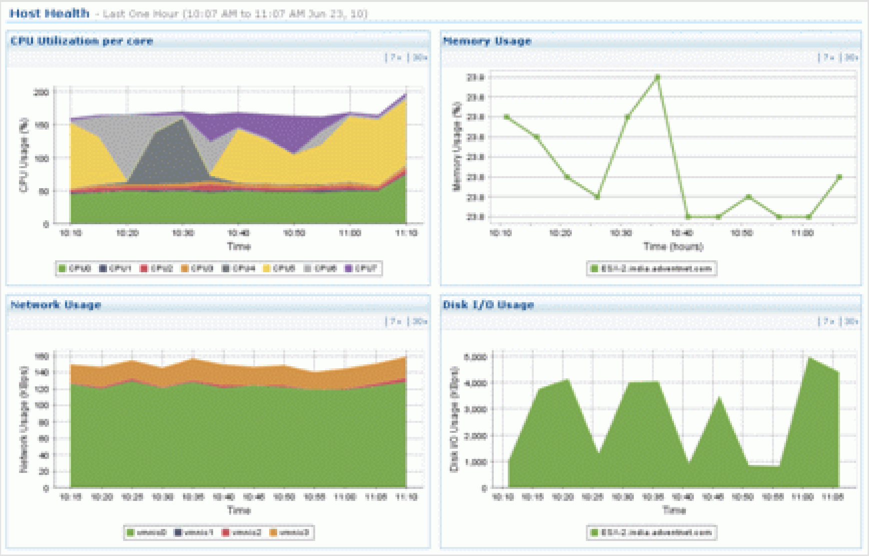
Host Details

ESX-2.india.adventnet.com

Virtual Entity Name	ESX-2.india.adventnet.com
IP Address	192.168.118.22
Vendor	VMware, Inc.
Version	4.0.0
CPU Cores	8 CPU x 2666 MHz
Processor Type	Intel(R) Xeon(R) CPU E5430 @ 2.66GHz
Memory Capacity	18430 MB
Logical Processors	8
Number of NICs	4
Number of HBAs	3
Connection State	connected
CPU Usage	4.67 GHz
Memory Usage	4.29 GB
Last SysUp Time	12:09 PM Jun 07, 10
Next Poll Time	11:11 AM Jun 23, 10
Passwords	Click here to change

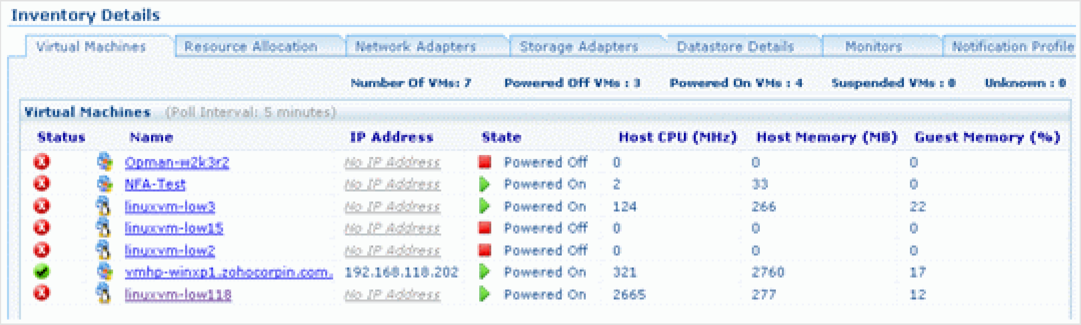
Host Heath At-a-Glance

This section provides the last one hour performance chart of the Host. You can view the reports of last 7 or 30 days. Click on 7 or 30 link available on the top right corner to view the last 7 or 30 days performance report respectively.



VM List & Resource Allocation Details

This section lists all the VMs on the Host, resources allotted to each VM, network adapters, storage adapters and datastore details. Any change in the inventory, gets updated automatically. You can also find the monitors that are enabled on the Host and notification profiles associated to it. Click on the respective tab to view its details.


Inventory Details

Number Of VMs: 7 Powered Off VMs : 3 Powered On VMs : 4 Suspended VMs : 0 Unknown : 0

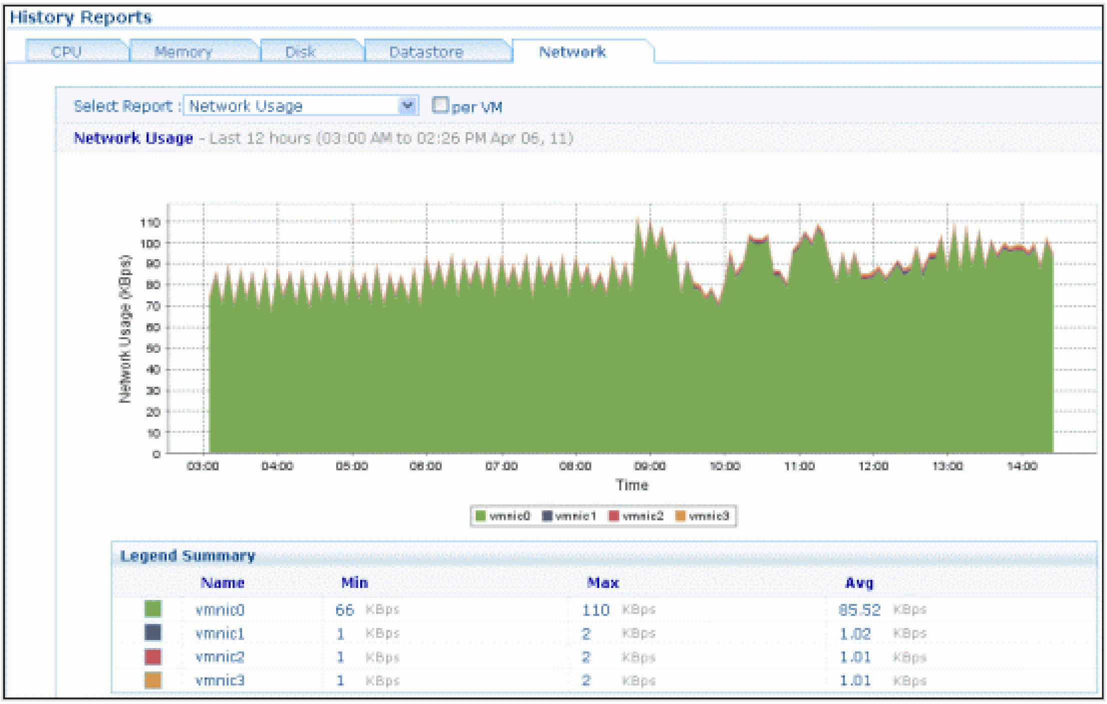
Virtual Machines (Poll Interval: 5 minutes)

Status	Name	IP Address	State	Host CPU (MHz)	Host Memory (MB)	Guest Memory (%)
☒	Opman-w2k3r2	No IP Address	Powered Off	0	0	0
☒	NFA-Test	No IP Address	Powered On	2	33	0
☒	linuxvm-low3	No IP Address	Powered On	124	266	22
☒	linuxvm-low15	No IP Address	Powered Off	0	0	0
☒	linuxvm-low2	No IP Address	Powered Off	0	0	0
✓	vmhp-winxp1.zohocorpin.com.	192.168.118.202	Powered On	321	2760	17
☒	linuxvm-low118	No IP Address	Powered On	2665	277	12

Click on the VM name to see its snapshot page. The snapshot page of the VM is similar to that of any Windows or Linux Server's snapshot page.

History Reports

OpManager also provides last 12 hour report on CPU, Memory, Disk, Datastore, and Network usage. Select the required report from the Select Report drop-down menu. If you want to view the utilization report for each VM, select the per VM check box.



Select Report : Network Usage ☐ per VM

Network Usage - Last 12 hours (03:00 AM to 02:26 PM Apr 06, 11)

Legend Summary

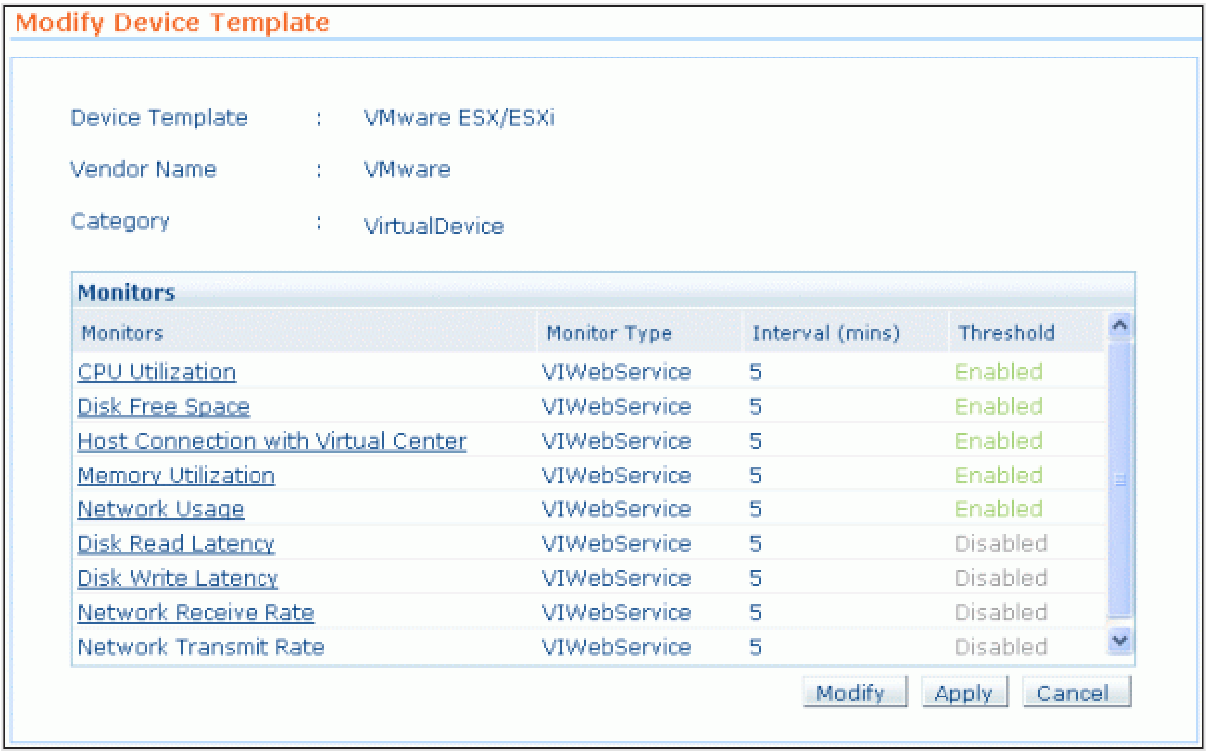
	Name	Min		Max		Avg	
🟩	vmnic0	66	KBps	110	KBps	85.52	KBps
🟦	vmnic1	1	KBps	2	KBps	1.02	KBps
🟥	vmnic2	1	KBps	2	KBps	1.01	KBps
🟧	vmnic3	1	KBps	2	KBps	1.01	KBps

Configuring Thresholds for VMware ESX and VMs

OpManager out-of-the-box offers monitoring templates for ESX hosts and VMs. The templates help you configure thresholds for multiple ESX hosts and VMs at one shot. For each performance metric you can configure Warning Threshold as well as Error Threshold, and receive proactive alerts if they are violated.

To configure the threshold value and apply the template

1. Go to **Admin**-> **Device Templates** and click on **V**.
2. You can find the **VMware ESX/ESXi** and **VMware Virtual Machine** templates for the hosts and VMs respectively. Click on the required template.



Modify Device Template

Device Template : VMware ESX/ESXi

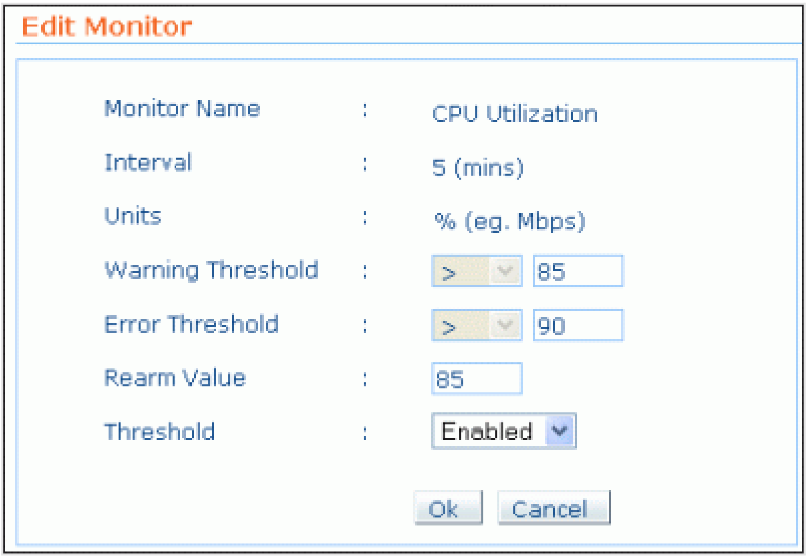
Vendor Name : VMware

Category : VirtualDevice

Monitors

Monitors	Monitor Type	Interval (mins)	Threshold
CPU Utilization	VIWebService	5	Enabled
Disk Free Space	VIWebService	5	Enabled
Host Connection with Virtual Center	VIWebService	5	Enabled
Memory Utilization	VIWebService	5	Enabled
Network Usage	VIWebService	5	Enabled
Disk Read Latency	VIWebService	5	Disabled
Disk Write Latency	VIWebService	5	Disabled
Network Receive Rate	VIWebService	5	Disabled
Network Transmit Rate	VIWebService	5	Disabled

3. Click on the monitor name to enable or disable the threshold, and to modify Warning Threshold, Error Threshold and Rearm Values.



Edit Monitor

Monitor Name : CPU Utilization

Interval : 5 (mins)

Units : % (eg. Mbps)

Warning Threshold : > 85

Error Threshold : > 90

Rearm Value : 85

Threshold : Enabled

4. Click **OK**.

5. Click **Modify** to modify the template.
6. Click **Apply** for the devices to inherit the configurations in the template. Or, click **Apply & Overwrite** for the devices to remove the old and add the new configurations in the template.

Note: To edit the threshold values of a single ESX host, go its snapshot page and click the Monitors tab under Inventory Details. Click on the Edit icon of a monitor to edit its threshold values.

Managing VMware Alerts

OpManager fetches events from each ESX Host, similar to SNMP traps. Currently we support important events, and this list is updated every release. Apart from host events, OpManager also monitors threshold for critical performance indicators and raises alerts. The complete list of threshold violation alerts and supported events are shown below in Table 1 and Table 2 respectively.

To change the pre-set threshold values for each performance monitor, go to the snapshot page of the host or VM. For the hosts, check for Inventory Details-> Monitors section. For VMs, check for Monitors-> VM Performance Monitors. All the VM specific performance monitors are grouped under 'VM Performance Monitors'.

Table 1: List of Threshold Monitors for critical performance indicators supported by OpManager

S.No.	Threshold Monitors	Virtual Device Type	Resource	Severity
1.	Host connection Status	Host	General	=2 (notresponding) - Critical =1 (disconnected) - Warning
2.	Host Data Received (avg)	Host	Network	>1000000 KBps - Critical >800000 KBps - Warning
3.	Host Data Transmission (avg)	Host	Network	>1000000 KBps - Critical >800000 KBps - Warning
4.	Host Network Usage (avg)	Host	Network	>4000000 KBps - Critical >3600000 KBps - Warning
5.	Host CPU Utilization (avg)	Host	CPU	> 90% - Critical > 85% - Warning
6.	Host Memory Utilization (avg)	Host	Memory	> 90% - Critical > 85% - Warning
7.	Host Disk Read Latency	Host	Disk	> 50ms - Critical > 45ms - Warning
8.	Host Disk Write Latency	Host	Disk	> 50ms - Critical > 45ms - Warning
9.	Datastore Freespace	Host	Network	< 5GB - Critical < 10GB - Warning
10.	VirtualMachine Data Received (avg)	VM	Network	>125000 KBps - Critical >100000 KBps - Warning
11	VirtualMachine Data Transmitted (avg)	VM	Network	>125000 KBps - Critical >100000 KBps - Warning
12.	VirtualMachine Network Usage (avg)	VM	Network	>250000 KBps - Critical >200000 KBps - Warning
13.	VirtualMachine CPU Usage (avg)	VM	CPU	> 90% - Critical > 85% - Warning
14.	VirtualMachine Memory Usage (avg)	VM	Memory	> 90% - Critical > 85% - Warning

Table 2: List of ESX hosts' events supported by OpManager

S.No.	Events	Virtual Device Type	Severity
1.	VmFailedToPowerOffEvent	VM	Major (Cleared on event 2 or 3)
2.	VmPoweredOffEvent	VM	Clear
3.	VmPowerOffOnIsolationEvent	VM	Clear
4.	VmFailedToPowerOnEvent	VM	Major (Cleared on event 5)
5.	VmPoweredOnEvent	VM	Clear
6.	VmFailedToSuspendEvent	VM	Major (Cleared on event 7)
7.	VmSuspendedEvent	VM	Clear
8.	VmFailedToRebootGuestEvent	VM	Major (Cleared on event 9)

9.	VmGuestRebootEvent	VM	Clear
10.	VmFailoverFailed	VM	Critical (Cleared on event 11)
11	VmPrimaryFailoverEvent	VM	Clear
12.	VmUpgradeFailedEvent	VM	Major (Cleared on event 13)
13.	VmUpgradeCompleteEvent	VM	Clear
14.	VmDisconnectedEvent	VM	Warning (Cleared on event 15)
15.	VmConnectedEvent	VM	Clear
16.	VmDiskFailedEvent	VM	Major
17.	VmRelocatedEvent	VM	Clear
18.	VmRelocateFailedEvent	VM	Critical (Cleared on event 17)

Notifying VMware Alerts

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert / email alert/ running a script etc. You can associate any of the notification profiles that is already created for the ESX host. Click here to create one new, . To associate a notification profile to a virtual device,

1. Go to the snapshot page of the host.
2. Scroll down to the Inventory Details section and click on **Notification Profiles** tab.
3. A link is shown if no profiles are associated. Click on the link to view the list of notification profiles already created.
4. Select the notification profile that you want to associate and click **Next**.
5. Select the check box "**when any [selected...] Virtual Device has problem**". It has two categories. General Alerts - alerts fetched from ESX host and Threshold Alerts raised when a performance metric violates a set threshold value.
6. Now select the alarms for which you want to be notified and click **Next**.
7. Select the time period for which you want to apply this profile and click **Next**.

- Apply this all time: The notification profile stays active 24x7
- Apply this profile during the below mentioned time window: The notification profile stays active only during the mentioned time interval and days. Eg. 09:00 to 20:00 - Monday to Friday

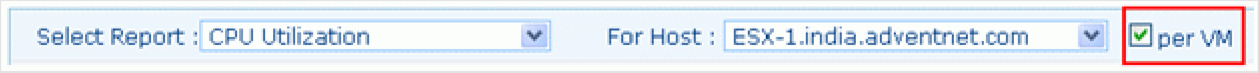
- Click **Save**.
- The notification profile is successfully associated to the host.

Accessing VMware Performance Reports

OpManager monitors all the critical parameters of your VMware servers and allows you to generate reports on the collected value. It provides over 70 different reports out-of-the-box, helping you get an insight into the performance trend and top hosts and VMs. All these reports are grouped under host reports & Virtual Machines reports. Further, they are subdivided based on system resources such as CPU, Memory, Network & Disk. The complete list of reports supported by OpManager is given in Table 3 for reference.

Host Reports:

View the reports for resources such as CPU, Memory, Network & Disk. Moreover, OpManager offers views to compare the performance of each VMs in a host. Say for example, when you see a gradual rise in Host CPU utilization trend, it would be useful to know which VM got affected due to the rise in physical resource. This information helps you quickly identify and fix the problem. With OpManager, you can select 'per VM' view (refer the screenshot given below) to compare the performance of VMs in that host.



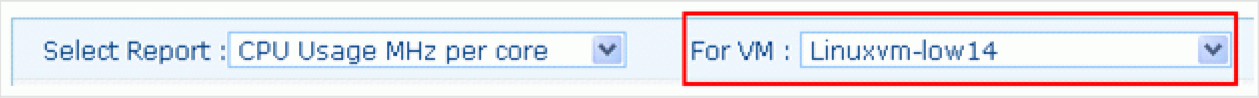
Select Report : CPU Utilization

For Host : ESX-1.india.adventnet.com

☑ per VM

VM Reports:

VM Reports offer reports for each individual VMs. Refer the screenshot given below.

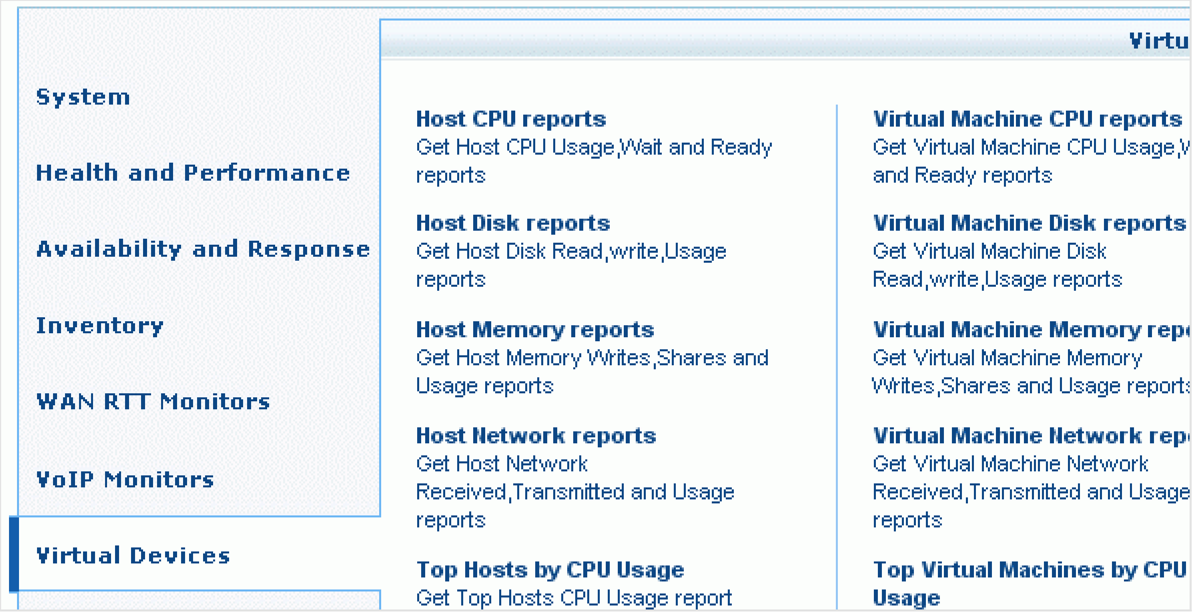


Select Report : CPU Usage MHz per core

For VM : Linuxvm-low14

Accessing Reports:

You can generate reports from the snapshot page or directly access the Reports tab. For ease of use, all the reports of the VMs and hosts are grouped under Virtual Devices category under the Reports tab. Click on the report name to generate the report.



Host CPU reports
Get Host CPU Usage,Wait and Ready reports

Host Disk reports
Get Host Disk Read,write,Usage reports

Host Memory reports
Get Host Memory Writes,Shares and Usage reports

Host Network reports
Get Host Network Received,Transmitted and Usage reports

Top Hosts by CPU Usage
Get Top Hosts CPU Usage report

Virtual Machine CPU reports
Get Virtual Machine CPU Usage,W and Ready reports

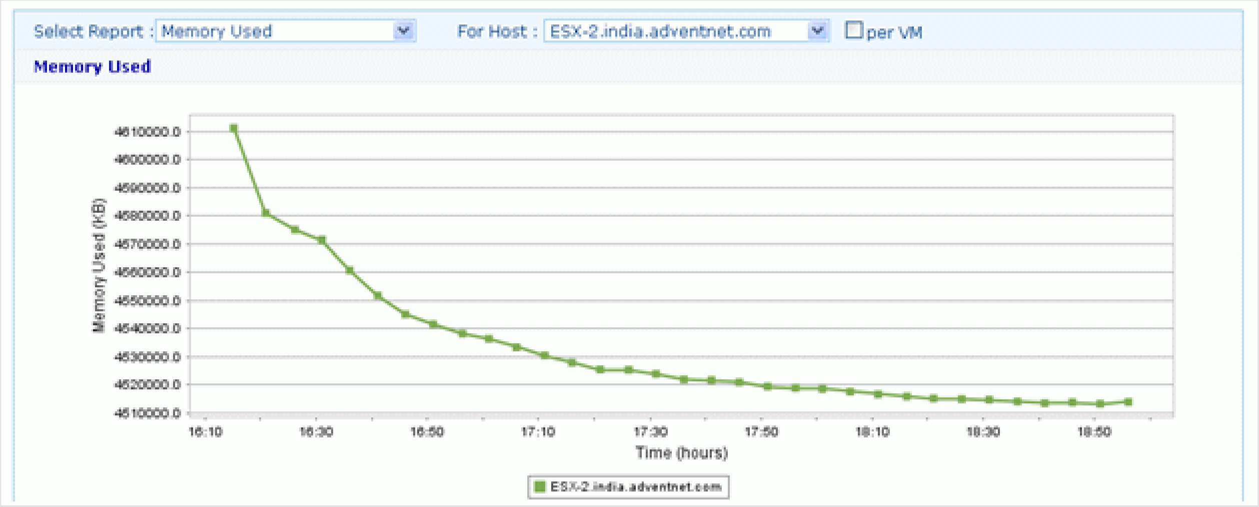
Virtual Machine Disk reports
Get Virtual Machine Disk Read,write,Usage reports

Virtual Machine Memory rep
Get Virtual Machine Memory Writes,Shares and Usage report

Virtual Machine Network rep
Get Virtual Machine Network Received,Transmitted and Usage reports

Top Virtual Machines by CPU Usage

Example: The screenshot below shows the memory used report for a host. You can select the required performance report from the Select Report dropdown menu. If you wish to view the report for another host, select the required host from For Host dropdown menu. To view the amount of memory used by each VM, select the per VM check box.



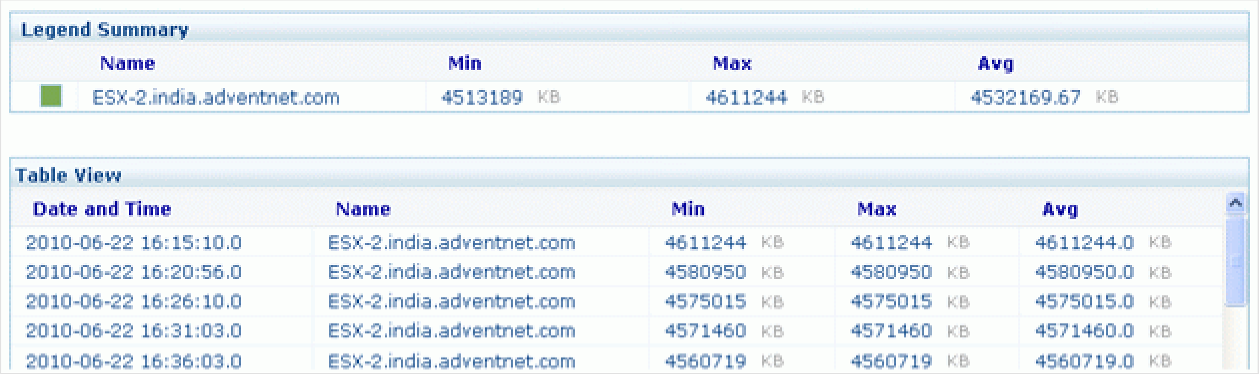
Select Report : Memory Used

For Host : ESX-2.india.adventnet.com

□ per VM

Memory Used

The screenshot below shows the legend summary and table view. Legend summary provides the minimum, maximum and average values of memory used by the host. Table view provides the same values collected during the recent polls.



Legend Summary

	Name	Min	Max	Avg
🟩	ESX-2.india.adventnet.com	4513189 KB	4611244 KB	4532169.67 KB

Table View

Date and Time	Name	Min	Max	Avg
2010-06-22 16:15:10.0	ESX-2.india.adventnet.com	4611244 KB	4611244 KB	4611244.0 KB
2010-06-22 16:20:56.0	ESX-2.india.adventnet.com	4580950 KB	4580950 KB	4580950.0 KB
2010-06-22 16:26:10.0	ESX-2.india.adventnet.com	4575015 KB	4575015 KB	4575015.0 KB
2010-06-22 16:31:03.0	ESX-2.india.adventnet.com	4571460 KB	4571460 KB	4571460.0 KB
2010-06-22 16:36:03.0	ESX-2.india.adventnet.com	4560719 KB	4560719 KB	4560719.0 KB

The reports can be exported to PDF or XLS format. You can also schedule reports and email them.

Table 3: Out-of-the-box reports that are offered by OpManager

S.No.	Report	Virtual Device Type	System Resource	Description
1	CPU Utilization per core	Host	CPU	Percentage (%) of actively used CPU of the Host per core
2	CPU Used	Host	CPU	Amount of time (in Milliseconds) CPU used per core
3	CPU Idle	Host	CPU	Amount of time (in Milliseconds) CPU is kept idle / unused.
4	CPU Overall Utilization	Host	CPU	Average CPU utilization of all cores, gives a quick overview of overall performance of the CPU in the host.
5	Memory Usage	Host	Memory	Percentage (%) of memory used of total configured memory.
6	Memory Used	Host	Memory	Average size (in KBytes) of memory used in overall
7	Memory Active	Host	Memory	Amount of memory (in KBytes) that is actively used
8	Memory Overhead	Host	Memory	Sum of overhead metrics for all powered-on virtual machines, and the overhead of running services on the host.
9	Memory Shared	Host	Memory	Sum of shared virtual memory of all powered-on VM's. This shared memory can be larger than the amount of machine memory available, if memory is over committed. This statistic reflects how effective transparent page sharing and memory overcommitment are saving machine memory.

10	Memory Shared Common	Host	Memory	Sum of shared machine memory by all powered-on VM's. Subtract this metric from the shared metric to calculate how much machine memory is saved due to sharing: shared - sharedcommon = machine memory (host physical memory) savings (KB)
11	Memory Swap In	Host	Memory	Sum of swapin values for all powered-on virtual machines on the host
12	Memory Swap Out	Host	Memory	Sum of swapout metrics from all powered-on virtual machines on the host
13	Memory Swap Used	Host	Memory	Sum of memory swapped of all powered on VM's
14	Network Usage	Host	Network	Sum of data transmitted and received (KBps) across all physical NIC instances connected to the Host
15	Network Received Speed	Host	Network	The rate (KBps) at which data is received across each physical NIC instance on the host.
16	Network Transmitted Speed	Host	Network	The rate (KBps) at which data is transmitted across each physical NIC instance on the host. VM: The rate at which data is transmitted across the VM's vNIC
17	Network Packets Received	Host	Network	Total number of packets received on all all physical NIC present on the host.
18	Network Packets Transmitted	Host	Network	Total number of packets transmitted across all physical NIC present in the host. VM:Number of packets transmitted by each vNIC on the VM
19	Disk I/O Usage	Host	Disk	Aggregated disk I/O rate. The rates for all virtual machines running on the host.
20	Disk Read Speed	Host	Disk	Rate (KBps) at which data is read for each LUN on the Host. Read Speed = (Number of blocksRead per second x blockSize)
21	Disk Write Speed	Host	Disk	Rate (KBps) at which data is written to each LUN on the Host
22	Disk Read Requests	Host	Disk	Number of times data was read from each LUN on the host
23	Disk Write Requests	Host	Disk	Number of times data was written to each LUN on the host
24	Disk Bus Resets	Host	Disk	Number of SCSI-bus reset commands issued
25	Disk Command Abort	Host	Disk	Number of SCSI commands aborted
26	Disk Read Latency	Host	Disk	Average amount of time (Milliseconds) to complete read from physical device
27	Disk Write Latency	Host	Disk	Average amount of time (Milliseconds) to complete write the physical device
28	Disk Space Usage	Host	Disk	Disk Space utilization for each Datastore
29	Top Hosts by CPU Usage	Host	CPU	List of Hosts by top CPU usage
30	Top Hosts by Memory Usage	Host	Memory	List of Hosts by top memory usage
31	Top Hosts by Swap Usage	Host	Memory	List of Hosts by top swap usage
32	Top Hosts by Network Usage	Host	Network	List of Hosts by top network usage
33	Top Hosts by Disk I/O Usage	Host	Disk	List of Hosts by top Disk I/O usage
34	Top Disk Space Consumers	Host	Disk	List of Hosts by top disk space consumption
35	CPU Usage MHz per core	VM	CPU	Amount of actively used virtual CPU per core
36	CPU Used	VM	CPU	Total amount of time (Milliseconds) CPU used
37	CPU Ready	VM	CPU	Total CPU time spent in ready state
38	CPU Wait	VM	CPU	Total CPU time spent in wait state
39	CPU Overall Utilization	VM	CPU	Average percentage of actively used virtual CPU on all cores, gives a overview of CPU performance of the VM.
40	Memory Usage	VM	Memory	Memory usage (%) of total configured memory for VM
41	Active Memory	VM	Memory	Amount of guest / VM memory actively used

42	Memory Balloon	VM	Memory	Amount of guest physical memory that is currently reclaimed from the virtual machine through ballooning. This is the amount of guest physical memory that has been allocated and pinned by the balloon driver. Note: You need to install the VMware tools on VM to use this feature. Installing VMware tools provides many more performance advantages, refer vmware website to read more about benefit of installing VMware tools.
43	Memory Overhead	VM	Memory	Amount of machine memory allocated to a virtual machine beyond its reserved amount, i.e., machine memory used by the VMkernel to run the virtual machine.
44	Memory Shared	VM	Memory	Amount of memory shared with other virtual machines
45	Memory Swapped	VM	Memory	Current amount of memory swapped out to the virtual machine's swap file by the VMkernel. Swapped memory stays on disk until the virtual machine needs it. This statistic refers to VMkernel swapping and not to guest OS swapping. swapped = swapin + swapout
46	Memory Consumed	VM	Memory	Amount of guest physical memory consumed by the virtual machine for guest memory. It includes shared memory and memory that might be reserved, but not actually used. Use this metric for charge-back purposes.
47	Network Usage	VM	Network	Sum of data transmitted and received across all virtual NIC instances connected to the virtual machine
48	Network Received Speed	VM	Network	The rate at which data is received across the virtual machine's vNIC (virtual network interface controller).
49	Network Transmitted Speed	VM	Network	The rate at which data is transmitted across the virtual machine's vNIC (virtual network interface controller).
50	Network Packets Received	VM	Network	The number of packets received by each vNIC (virtual network interface controller) on the virtual machine.
51	Network Packets Transmitted	VM	Network	Number of packets transmitted by each vNIC on the virtual machine.
52	Disk Read Speed	VM	Disk	Rate at which data is read from each virtual disk on the virtual machine
53	Disk Write Speed	VM	Disk	Rate at which data is written to each virtual disk on the virtual machine.
54	Disk Read Requests	VM	Disk	Number of times data was read from each virtual disk on the virtual machine
55	Disk Write Requests	VM	Disk	Number of times data was written to each virtual disk on the virtual machine
56	Disk Bus Resets	VM	Disk	Number of SCSI-bus reset commands issued
57	Top VMs by CPU Usage	VM	CPU	List of VMs by top CPU usage
58	Top VMs by CPU Ready	VM	CPU	List of VMs by top CPU Ready usage
59	Top VMs by Memory Usage	VM	Memory	List of VMs by top memory usage
60	Top VMs by Swap Usage	VM	Memory	List of VMs by top swap usage
61	Top VMs by Network Usage	VM	Network	List of VMs by top network usage
62	Top VMs by Disk I/O Usage	VM	Disk	List of VMs by top Disk I/O usage
63	Datastore Read Speed	Host	Datastore	Rate of reading data from the datastore by the host
64	Datastore Write Speed	Host	Datastore	Rate of writing data to the datastore by the host
65	Datastore Write Requests	Host	Datastore	Average number of write commands issued per second by the host to the datastore during the collection interval.
66	Datastore Read Requests	Host	Datastore	Average number of read commands issued per second by the host to the datastore during the collection interval.
67	Datastore Read Latency	Host	Datastore	Average amount of time for a read operation from the datastore
68	Datastore Write Latency	Host	Datastore	Average amount of time for a write operation from the datastore
69	Datastore Normalized Latency	Host	Datastore	Normalized latency in microseconds on the datastore. Data for all virtual machines is combined.

70	Datastore Aggregate number of IO Operations	Host	Datastore	Aggregate number of IO operations on the datastore.
71	Datastore Read Speed	VM	Datastore	Rate of reading data from the datastore by the VM
72	Datastore Write Speed	VM	Datastore	Rate of writing data to the datastore by the VM
73	Datastore Write Requests	VM	Datastore	Average number of write commands issued per second by the VM to the datastore during the collection interval.
74	Datastore Read Requests	VM	Datastore	Average number of read commands issued per second by the VM to the datastore during the collection interval.

Monitoring Hyper-V Host and VMs

OpManager monitors Hyper-V servers via WMI. It provides separate dashboard for Hosts and VMs, to have a quick view on its performance. It also offers a dedicated Snapshot page for the Hyper-V host, which provides comprehensive data such as Health, Inventory, Performance Reports, etc.

Some highlights of monitoring Hyper-V servers with OpManager:

- Monitors effective utilization of critical resources like CPU, Memory, Network and Disk
- Out-of-the-box offers 50 reports on Host and VMs
- Automatically maps the migrated VMs to the corresponding Hosts

Apart from monitoring the Hosts and VMs, OpManager also monitors the Key Performance Indicators (KPIs) of guest OSs. Similar to that of any Windows or Linux server, OpManager monitors the applications, Windows & TCP services, processes running on the VMs using WMI/SNMP.

Discovering Hyper-V Servers in OpManager

To discover the Hyper-V host and VMs, you just need to provide the IP address and WMI credentials of Hyper-V host. The VMs are automatically discovered along with the host.

Steps to discover the Hyper-V host and VMs:
Before proceeding to discover the host and VMs, ensure that you have configured the credentials for both the host and VMs in the credential library. To discover the host and VMs:

1. Go to **Admin**-> **Add Device**. (You can also access the Add Device window from **Maps**-> **Virtual Devices**-> **Add New Hyper-V Host**).
2. Enter the **Host Name / IP Address.**
3. Enter the correct **Netmask** and select the appropriate **credentials**.
4. Click **Add Device** button to add the host.

If any of the VMs are already discovered or added, OpManager automatically maps them as Virtual Device. Once the discovery is over you can find the Host & VMs under 'Virtualization' tab.

Note: If the device has been added successfully, but not displayed under the 'Virtualization' tab, search for that device. Go to its snapshot page and look for the device type. If it is mentioned as ‘unknown’, wrong credentials might have been provided or it is not reachable during discovery. Provide the correct credentials and click on ‘Rediscover Now’ under Actions tab in the snapshot page, to discover it as an Hyper-V host.

Monitoring Hyper-V servers

All the discovered hosts and VMs are mapped under 'Virtualization' tab to open the Virtual Devices dashboard page, which provides a quick glance of your critical resources such as CPU, Memory, Network & Disk that are under pressure. Though ideal resource utilization is the key benefit we get from virtualization, it can lead to other problems because it is shared among the servers. Even if a single system has a resource crunch, it hugely affects the performance of the other systems running on the same host. Quickly identifying and fixing the resource utilization problems is therefore vital for a business to run smooth.

OpManager shows the top hosts and VMs by resource utilization and the recent alarms raised. Click on the host or the VM name to see its snapshot page. The Virtual Devices Dashboard page refreshes automatically every 5 minutes to reflect the latest collected statistics.

Listed below are the various types of top resource utilization widgets to quickly identify any over utilized resource. It gives a quick glance on systems which are the top consumers of CPU, Memory, Network, Disk I/O and Disk Space.

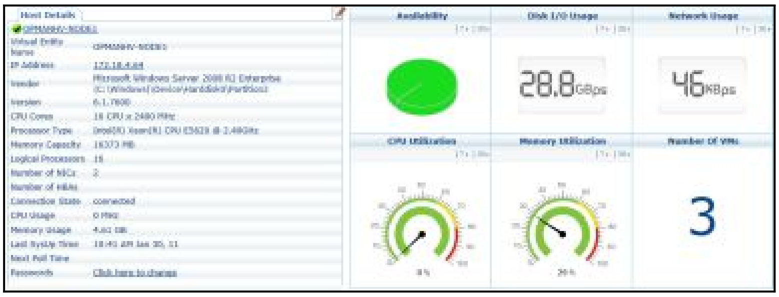
Top VMs	Top Hosts
1. Top CPU Consumers 2. Top CPU Ready Consumers 3. Top Memory Consumers 4. Top Swap Memory Consumers 5. Top Disk I/O Consumers 6. Top Network Consumers	1. Top CPU Consumers 2. Top Memory Consumers 3. Top Swap Memory Consumers 4. Top Network Consumers 5. Top Disk I/O Consumers 6. Top Disk Space Consumers

Snapshot page of a Host

Snapshot page of Host / VM provides a summary of the current statistics, recent alarms, configuration details such as VMs inventory, resource allocation for each VM, Network Adapters, Storage Adapters, Datastores, and much more.

Host Details and Performance Charts

In this section you can find the Host details like IP Address, Vendor of Host, CPU Cores etc. on the left side. The right side gives a quick glance on performance data like CPU Utilization, Memory Utilization, Disk I/O Usage etc., collected during the last poll. These values are collected at an interval of 5 minutes. These data help you determine the current performance of the Host.



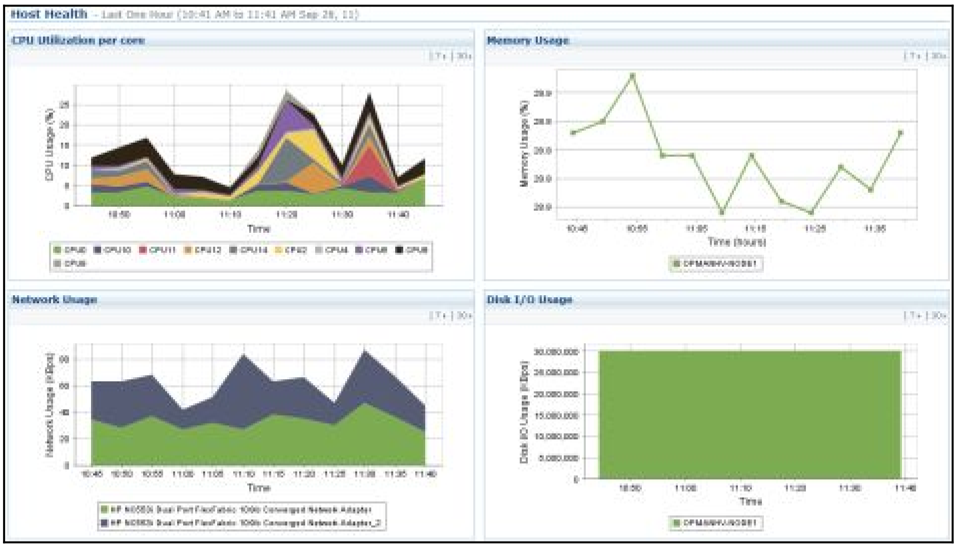
Host Details

OPMANHV-NODE1

Virtual Entity Name	OPMANHV-NODE1
IP Address	172.18.4.84
Vendor	Microsoft Windows Server 2008 R2 Enterprise (C:\Windows|\Device\Harddisk0\Partition1)
Version	6.1.7600
CPU Cores	16 CPU x 2480 MHz
Processor Type	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Memory Capacity	16373 MB
Logical Processors	16
Number of NICs	2
Number of HBAs	
Connection State	connected
CPU Usage	0 MHz
Memory Usage	4.61 GB
Last SysUp Time	10:41 AM Jan 30, 11
Next Poll Time	
Passwords	Click here to change

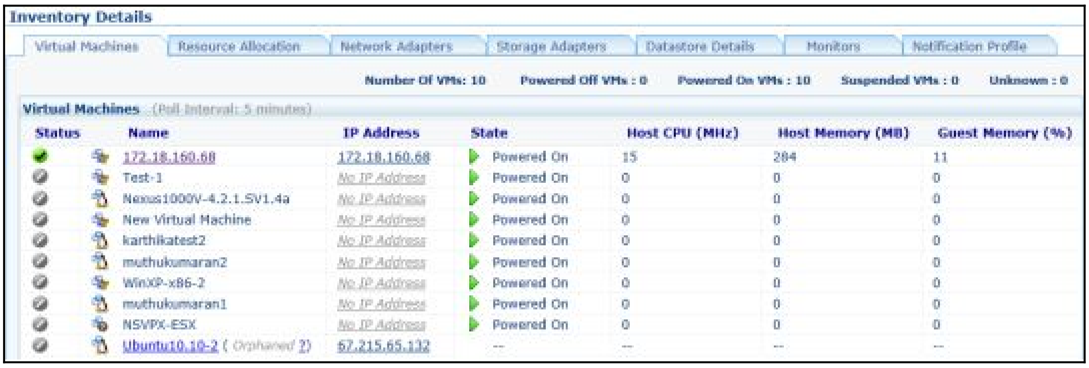
Host Heath At-a-Glance

This section provides the last one hour performance chart of the Host. You can view the reports of last 7 or 30 days. Click on 7 or 30 link available on the top right corner to view the last 7 or 30 days performance report respectively.



VM List & Resource Allocation Details

This section lists all the VMs on the Host, resources allotted to each VM, network adapters, storage adapters and datastore details. Any change in the inventory, gets updated automatically. You can also find the monitors that are enabled on the Host and notification profiles associated to it. Click on the respective tab to view its details.



Number Of VMs: 10 Powered Off VMs : 0 Powered On VMs : 10 Suspended VMs : 0 Unknown : 0

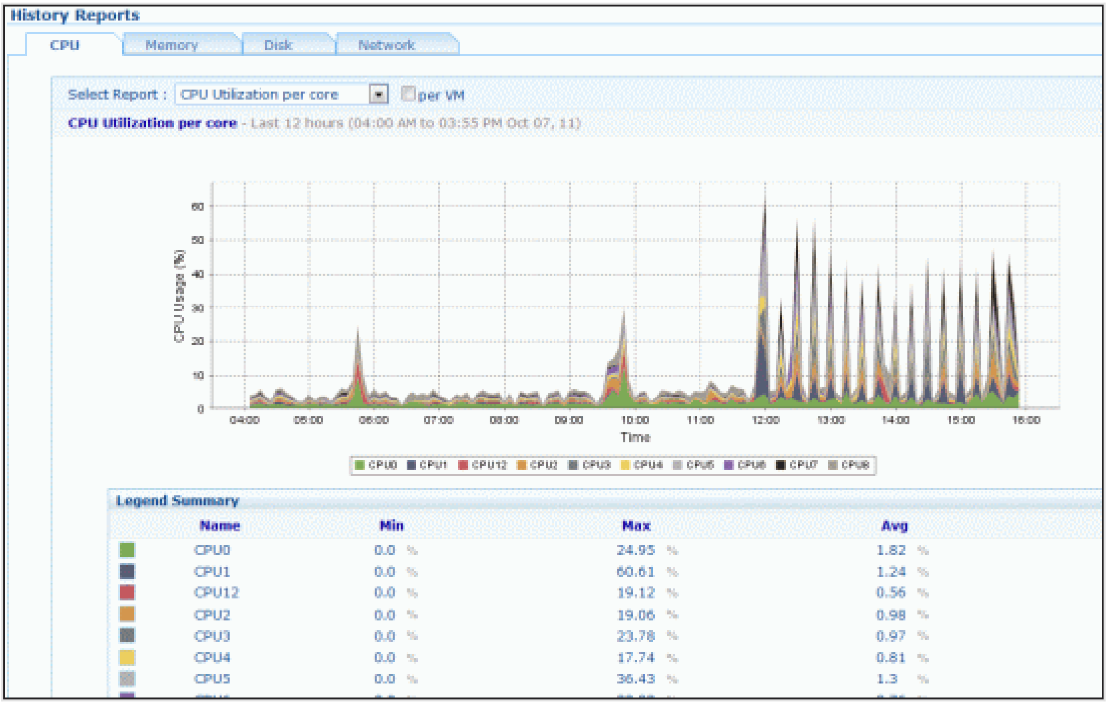
Virtual Machines (Poll Interval: 5 minutes)

Status	Name	IP Address	State	Host CPU (MHz)	Host Memory (MB)	Guest Memory (%)
✓	172.18.160.68	172.18.160.68	Powered On	15	284	11
●	Test-1	No IP Address	Powered On	0	0	0
●	Nexus1000V-4.2.1.SV1.4a	No IP Address	Powered On	0	0	0
●	New Virtual Machine	No IP Address	Powered On	0	0	0
●	karthikatest2	No IP Address	Powered On	0	0	0
●	muthukumaran2	No IP Address	Powered On	0	0	0
●	WinXP-x86-2	No IP Address	Powered On	0	0	0
●	muthukumaran1	No IP Address	Powered On	0	0	0
●	NSVPX-ESX	No IP Address	Powered On	0	0	0
●	Ubuntu10.10-2 (Orphaned ?)	67.215.65.132	--	--	--	--

Click on the VM name to see its snapshot page. The snapshot page of the VM is similar to that of any Windows or Linux Server's snapshot page.

History Reports

OpManager also provides last 12 hour report on CPU, Memory, Disk, and Network usage. Select the required report from the Select Report drop-down menu. If you want to view the utilization report for each VM, select the per VM check box.



History Reports

CPU | Memory | Disk | Network

Select Report : CPU Utilization per core ▾ □ per VM

CPU Utilization per core - Last 12 hours (04:00 AM to 03:55 PM Oct 07, 11)

Legend Summary

	Name	Min	Max	Avg
🟩	CPU0	0.0 %	24.95 %	1.82 %
⬛	CPU1	0.0 %	60.61 %	1.24 %
🟥	CPU12	0.0 %	19.12 %	0.56 %
🟧	CPU2	0.0 %	19.06 %	0.98 %
⬛	CPU3	0.0 %	23.78 %	0.97 %
🟨	CPU4	0.0 %	17.74 %	0.81 %
⬜	CPU5	0.0 %	36.43 %	1.3 %

Configuring Thresholds for Hyper-V Host and VMs

OpManager out-of-the-box offers monitoring templates for Hyper-V hosts and VMs. The templates help you configure thresholds for multiple hosts and VMs at one shot. The process is similar to that of configuring threshold to monitors available for Windows/Linux servers.

To configure the threshold value and apply the template

1. Go to **Admin**-> **Device Templates** and click on **H**.
2. You can find the **HyperVServer** and **HyperV-Virtual Machine** templates for the hosts and VMs respectively. Click on the required template.
3. Click on **Edit Threshold** button to configure the threshold and rearm value for the required monitors.
4. Click **OK**.
5. Click **Modify** to modify the template.
6. Click **Apply** for the devices to inherit the configurations in the template. Or, click **Apply & Overwrite** for the devices to remove the old and add the new configurations in the template.

Note: To edit the threshold values of a single host, go its snapshot page and click the Monitors tab under Inventory Details. Click on the Edit icon of a monitor to edit its threshold values.

Managing Hyper-V Alerts

OpManager monitors Hyper-V host and VM similar to that of any Windows server. Upon clicking the monitors tab in the host snapshot page, the monitors listed for a Windows server is listed here. You can add the required monitors and configure thresholds. If the threshold is violated, OpManager raises an alarm.

Notifying Hyper-V Alerts

Notification profiles help you to notify when any alert is raised for virtual devices. The notification can be a sound alert / email alert/ running a script etc. You can associate any of the notification profiles that is already created for the Hyper-V host. Click here to create one new. Associating notification profile to a Hyper-V host and VM are similar to that of associating a notification profile to a Windows server.

Accessing Hyper-V Performance Reports

OpManager monitors all the critical parameters of your Hyper-V servers and allows you to generate reports on the collected value. It provides 50 different reports out-of-the-box, helping you get an insight into the performance trend and top hosts and VMs. All these reports are grouped under host reports & Virtual Machines reports. Further, they are subdivided based on system resources such as CPU, Memory, Network & Disk. The complete list of reports supported by OpManager is given in Table 4 for reference.

Host Reports:

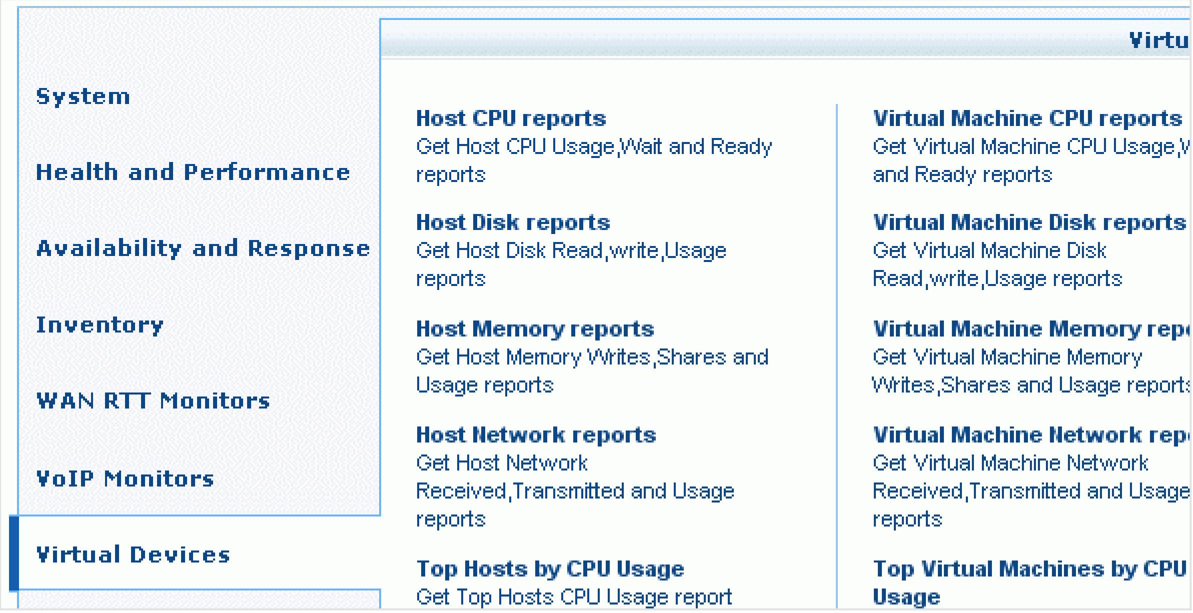
View the reports for resources such as CPU, Memory, Network & Disk, under History reports, in the host snapshot page. Moreover, OpManager offers views to compare the performance of each VMs in a host. Say for example, when you see a gradual rise in Host CPU utilization trend, it would be useful to know which VM got affected due to the rise in physical resource. This information helps you quickly identify and fix the problem. With OpManager, you can select 'per VM' view check box to compare the performance of VMs in that host.

VM Reports:

Similar to viewing reports for resources such as CPU, Memory, Network & Disk of a host, you can also view such reports for every VM in its snapshot page.

Accessing Reports:

You can generate reports from the snapshot page or directly access the Reports tab. For ease of use, all the reports of the VMs and hosts are grouped under Virtual Devices category under the Reports tab. Click on the report name to generate the report.



Host CPU reports
Get Host CPU Usage,Wait and Ready reports

Host Disk reports
Get Host Disk Read,write,Usage reports

Host Memory reports
Get Host Memory Writes,Shares and Usage reports

Host Network reports
Get Host Network Received,Transmitted and Usage reports

Top Hosts by CPU Usage
Get Top Hosts CPU Usage report

Virtual Machine CPU reports
Get Virtual Machine CPU Usage,W and Ready reports

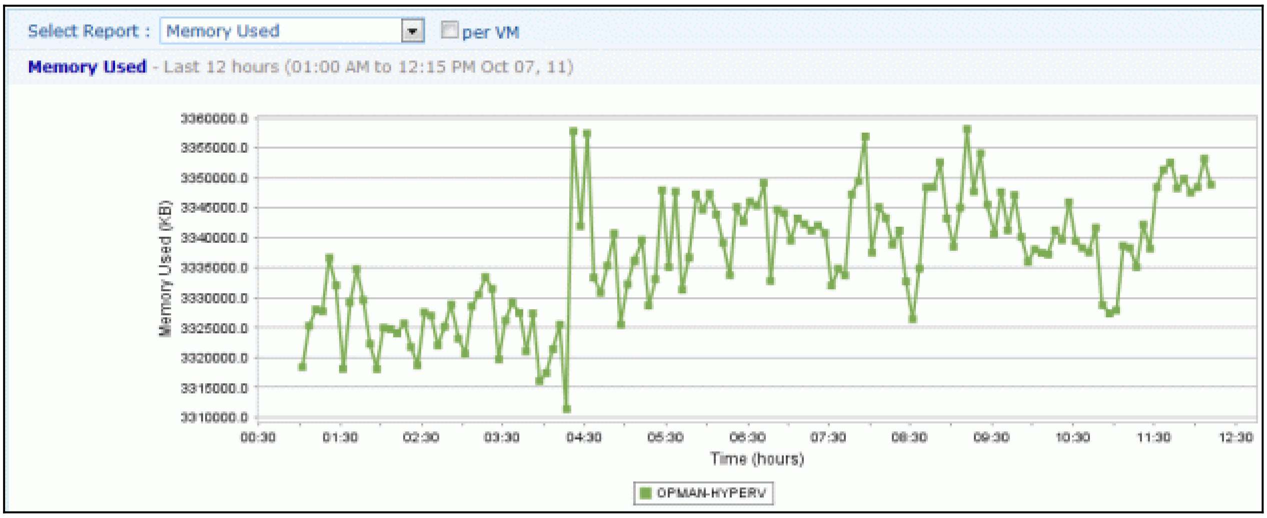
Virtual Machine Disk reports
Get Virtual Machine Disk Read,write,Usage reports

Virtual Machine Memory repo
Get Virtual Machine Memory Writes,Shares and Usage reports

Virtual Machine Network repo
Get Virtual Machine Network Received,Transmitted and Usage reports

Top Virtual Machines by CPU Usage

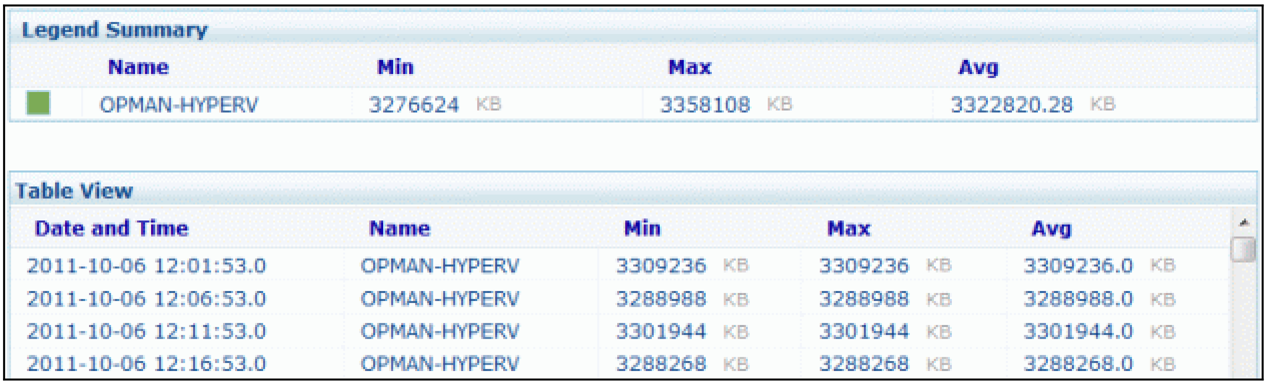
Example: The screenshot below shows the memory used report for a host. You can select the required performance report from the Select Report dropdown menu. If you wish to view the report for another host, go to its snapshot page and select the required requried report. To view the amount of memory used by each VM, select the per VM check box.



Select Report : Memory Used ▾ □ per VM

Memory Used - Last 12 hours (01:00 AM to 12:15 PM Oct 07, 11)

The screenshot below shows the legend summary and table view. Legend summary provides the minimum, maximum and average values of memory used by the host. Table view provides the same values collected during the recent polls.



Legend Summary

	Name	Min	Max	Avg
🟩	OPMAN-HYPERV	3276624 KB	3358108 KB	3322820.28 KB

Table View

Date and Time	Name	Min	Max	Avg
2011-10-06 12:01:53.0	OPMAN-HYPERV	3309236 KB	3309236 KB	3309236.0 KB
2011-10-06 12:06:53.0	OPMAN-HYPERV	3288988 KB	3288988 KB	3288988.0 KB
2011-10-06 12:11:53.0	OPMAN-HYPERV	3301944 KB	3301944 KB	3301944.0 KB
2011-10-06 12:16:53.0	OPMAN-HYPERV	3288268 KB	3288268 KB	3288268.0 KB

The reports can be exported to PDF or XLS format. You can also schedule reports and email them.

Table 4: Out-of-the-box reports that are offered by OpManager

S.No.	Report	Virtual Device Type	System Resource	Description
1	CPU Utilization per core	Host	CPU	Percentage (%) of actively used CPU of the Host per core
2	CPU Used	Host	CPU	Amount of time (in Milliseconds) CPU used per core
3	CPU Idle	Host	CPU	Amount of time (in Milliseconds) CPU is kept idle / unused.
4	CPU Overall Utilization	Host	CPU	Average CPU utilization of all cores, gives a quick overview of overall performance of the CPU in the host.
5	Memory Usage	Host	Memory	Percentage (%) of memory used of total configured memory.
6	Memory Used	Host	Memory	Average size (in KBytes) of memory used in overall
7	Memory Active	Host	Memory	Amount of memory (in KBytes) that is actively used
8	Network Usage	Host	Network	Sum of data transmitted and received (KBps) across all physical NIC instances connected to the Host
9	Network Received Speed	Host	Network	The rate (KBps) at which data is received across each physical NIC instance on the host.
10	Network Transmitted Speed	Host	Network	The rate (KBps) at which data is transmitted across each physical NIC instance on the host. VM: The rate at which data is transmitted across the VM's vNIC
11	Network Packets Received	Host	Network	Total number of packets received on all all physical NIC present on the host.

12	Network Packets Transmitted	Host	Network	Total number of packets transmitted across all physical NIC present in the host. VM:Number of packets transmitted by each vNIC on the VM
13	Disk I/O Usage	Host	Disk	Aggregated disk I/O rate. The rates for all virtual machines running on the host.
14	Disk Read Speed	Host	Disk	Rate (KBps) at which data is read for each LUN on the Host. Read Speed = (Number of blocksRead per second x blockSize)
15	Disk Write Speed	Host	Disk	Rate (KBps) at which data is written to each LUN on the Host
16	Disk Read Requests	Host	Disk	Number of times data was read from each LUN on the host
17	Disk Write Requests	Host	Disk	Number of times data was written to each LUN on the host
18	Disk Read Latency	Host	Disk	Average amount of time (Milliseconds) to complete read from physical device
19	Disk Write Latency	Host	Disk	Average amount of time (Milliseconds) to complete write the physical device
20	Disk Space Usage	Host	Disk	Disk Space utilization for each Datastore
21	Top Hosts by CPU Usage	Host	CPU	List of Hosts by top CPU usage
22	Top Hosts by Memory Usage	Host	Memory	List of Hosts by top memory usage
23	Top Hosts by Swap Usage	Host	Memory	List of Hosts by top swap usage
24	Top Hosts by Network Usage	Host	Network	List of Hosts by top network usage
25	Top Hosts by Disk I/O Usage	Host	Disk	List of Hosts by top Disk I/O usage
26	Top Disk Space Consumers	Host	Disk	List of Hosts by top disk space consumption
27	CPU Usage MHz per core	VM	CPU	Amount of actively used virtual CPU per core
28	CPU Used	VM	CPU	Total amount of time (Milliseconds) CPU used
29	CPU Ready	VM	CPU	Total CPU time spent in ready state
30	CPU Wait	VM	CPU	Total CPU time spent in wait state
31	**CPU Utilization**	VM	CPU	Average percentage of actively used virtual CPU on all cores, gives a overview of CPU performance of the VM.
32	Memory Usage	VM	Memory	Memory usage (%) of total configured memory for VM
33	Active Memory	VM	Memory	Amount of guest / VM memory actively used
34	Memory Overhead	VM	Memory	Amount of machine memory allocated to a virtual machine beyond its reserved amount, i.e., machine memory used by the VMkernel to run the virtual machine.
35	Memory Consumed	VM	Memory	Amount of guest physical memory consumed by the virtual machine for guest memory. It includes shared memory and memory that might be reserved, but not actually used. Use this metric for charge-back purposes.
36	Network Usage	VM	Network	Sum of data transmitted and received across all virtual NIC instances connected to the virtual machine
37	Network Received Speed	VM	Network	The rate at which data is received across the virtual machine's vNIC (virtual network interface controller).
38	Network Transmitted Speed	VM	Network	The rate at which data is transmitted across the virtual machine's vNIC (virtual network interface controller).
39	Network Packets Received	VM	Network	The number of packets received by each vNIC (virtual network interface controller) on the virtual machine.
40	Network Packets Transmitted	VM	Network	Number of packets transmitted by each vNIC on the virtual machine.
41	Disk Read Speed	VM	Disk	Rate at which data is read from each virtual disk on the virtual machine
42	Disk Write Speed	VM	Disk	Rate at which data is written to each virtual disk on the virtual machine.
43	Disk Read Requests	VM	Disk	Number of times data was read from each virtual disk on the virtual machine
44	Disk Write Requests	VM	Disk	Number of times data was written to each virtual disk on the virtual machine
45	Top VMs by CPU Usage	VM	CPU	List of VMs by top CPU usage
46	Top VMs by CPU Ready	VM	CPU	List of VMs by top CPU Ready usage
47	Top VMs by Memory Usage	VM	Memory	List of VMs by top memory usage

48	Top VMs by Swap Usage	VM	Memory	List of VMs by top swap usage
49	Top VMs by Network Usage	VM	Network	List of VMs by top network usage
50	Top VMs by Disk I/O Usage	VM	Disk	List of VMs by top Disk I/O usage

About VoIP Monitor

Cisco IPSLA monitor or VoIP monitor comes as an add-on feature in OpManager and requires licenese to run. OpManager continuously monitors the key performance metrics of the VoIP network to determine its health. The parameters measured include Jitter, Latency, Packet Loss, etc.

Jitter: Jitter indicates a variation in delay between arriving packets (inter-packet delay variance). Users often experience uneven gaps in speech pattern of the person talking on the other end, and sometimes there are disturbing sounds over a conversation coupled with loss of synchronization etc.

Latency: The delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site is called as latency. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

Packet Loss : Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency.

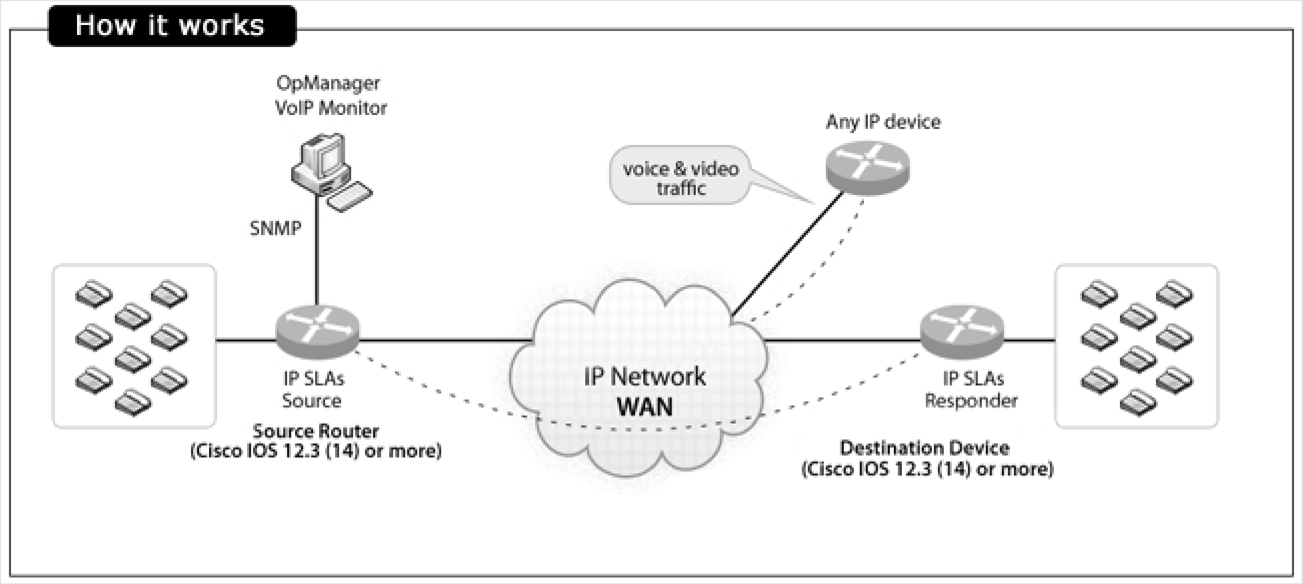
MOS: The jitter codec determines the quality of VoIP traffic and each codec provides a certain quality of speech. The Mean Opinion Score is a standard for measuring voice codecs and is measured in the scale of 1 to 5 (poor quality to perfect quality). The quality of transmitted speech is a subjective response of the listener.

How it works

OpManager primarily relies on Cisco's IP-SLA for monitoring the VoIP and the prerequisite therefore is, that the device should be a Cisco Router and must have IPSLA agent enabled on it. From IOS Version 12.3(14)T all Cisco routers support monitoring of VoIP QoS metrics.

Cisco's IPSLA, an active monitoring feature of Cisco IOS software, facilitates simulating and measuring the above mentioned parameters to ensure that your SLAs are met.

Cisco IP SLA provides a UDP jitter operation where UDP packets are sent from the source device to a destination device. This simulated traffic is used to determine the jitter, the round-trip-time, packet loss and latency. This data is gathered for multiple tests over a specified period to identify how the network performs at different times in a day or over a few days. The VoIP monitor gathers useful data that helps determine the performance of your VoIP network, equipping you with the required information to perform network performance assessment, troubleshooting, and continuous health monitoring.



Adding a New VoIP Monitor

Prerequisites

When you want to test a link from your office to another location, you need a Cisco router (IOS version 12.4 or later) at each end.

Steps to set up the monitor

Using OpManager, you can now monitor the voice and video quality of a 'call path'. Call path is the WAN link between the router in your main office and the one in the branch office that you want to monitor.

Step 1 : Enable Add (/discover) the router in your LAN to OpManager. And make sure the SNMP read and write community are configured properly, for that router.

Step 2: Enable SLA responder on the destination device you wish to monitor, Steps are detailed below.

a. Open a CLI session on the destination router and enable the EXEC mode as follows:

   Router>enable

b. Start the global configuration mode:

   Router#configure terminal

c. Enable the IP SLA responder:

   Router(config)#ip sla responder
   [or]
   Router(config)#ip sla monitor responder
   (Note: Enter any one of the command to enable IP SLA responder as it varies according to the IOS versions.)

d. Repeat the above steps for all the destination routers on which you want to monitor VoIP performance.

Step 3: Creating the VoIP monitor:

a. Go to Home-> VoIP Monitors->Configure VoIP Monitor-> Create New, and enter a name for the monitor.
b. Select the source router from the list of routers discovered in OpManager, and select the relevant interface.
c. Specify the destination router either by using the 'Search' option to pick from the discovered routers, or use the 'Add' option to specify the IP address of the destination router and submit the details.
d. You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure.
   Refresh the page after few seconds to see the new monitor. The data will be collected every hour, from the time you have configured.

[or]

You can also create the VoIP monitor from the Router snapshot page. To do so, go to Router snapshot page, click on Action tab and select Add VoIP Monitor. Enter the Monitor Name and Destination IP. Click Submit to create the monitor or Click Advanced button to go to Create New VoIP Monitor page and follow the steps from 2 to 4 given under Step 3.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration. Go through the FAQs section to understand QoS parameters.

Configuring call settings and threshold template

Defining Call Settings:

Define a template with the required VoIP settings to be used for monitoring performance. The VoIP template comes with pre-populated default values. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows:

1. Mouse-over Maps tab and click VoIP Monitors.
2. Go to Settings-> Call Settings.
3. Configure the following parameters:

Destination Port - Specify the VoIP UDP port to which VoIP Monitor sends simulated traffic to generate performance metrics. The default port number is set as 16384. You can specify a port in the range of 16384 - 32766.

Simulated VoIP Codec - The VoIP jitter codec decides the type of traffic that VoIP Monitor simulates over your network.

Operation Frequency - The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.

Operation Timeout - The operation timeout is time to wait for the response from the responder / destination device in msecs.

Type of service - The Type of Service octet allows you to set precedence levels for VoIP traffic of the IP SLA operations.

MOS Advantage Factor - The advantage factor is a measure, on a scale of 0 to 20, of the willingness of your VoIP network users to trade call quality for convenience

Defining Thresholds for the monitored parameters:

You can define a threshold template so that the VoIP performance parameters can be better suit your company SLA's (Service Level Agreements). Alerts are triggered based on the thresholds configured so that you can take corrective actions in time. Here are the steps to define a threshold template:

1. Mouse-over Maps tab and click VoIP Monitors.
2. Go to Settings->Threshold Template.
3. Configure the following values:

MOS Threshold : Configure the MOS threshold by specifying the upper and lower MOS range values in the range of 1 to 5.

Jitter Threshold : Configure the jitter threshold in msecs with upper and lower threshold limits. The range is from 0 to 6000 msecs.

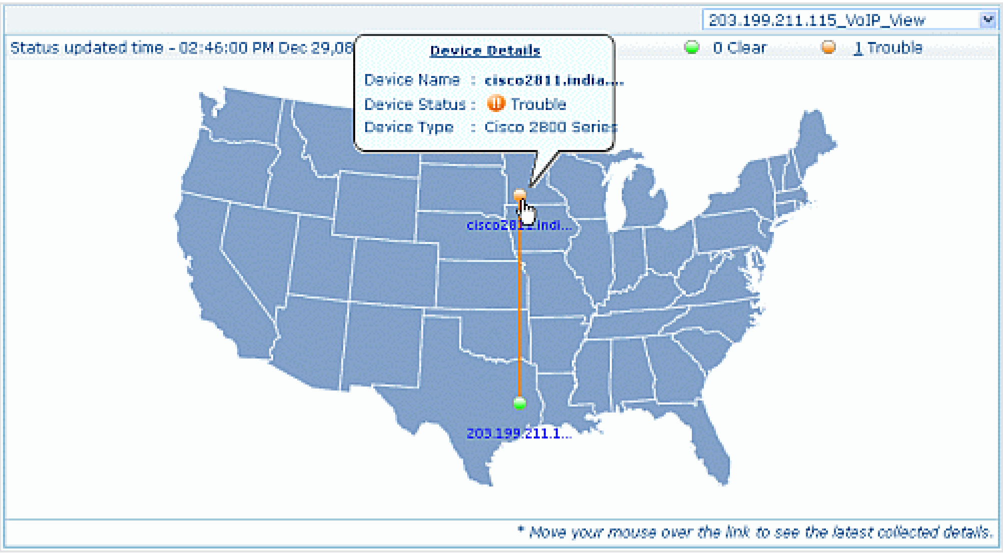
Latency Threshold : Specify the delay allowed in msecs again in the range of 0 to 6000.

Packet Loss : Specify the number of packets that can be lost in transit.

Notification Profile : Select the required notification profile(s) in order to notify when the any threshold rule is violated.

Business Views in VoIP Monitor

In VoIP Monitor, business views help you to know the status of the device and call path between devices at a glance. Whenever a new VoIP monitor is created, a business view (image shown below) of it also gets created automatically with the default background and device icons. However, later you can modify the background and device icons if required.


203.199.211.115_VoIP_View
Status updated time - 02:46:00 PM Dec 29,08
Device Details
Device Name : cisco2811.india....
Device Status : Trouble
Device Type : Cisco 2800 Series
0 Clear
1 Trouble
cisco2811.indi...
203.199.211.1...
* Move your mouse over the link to see the latest collected details.

In the business view, mouse-over the device icon or name/IP and call path to view its details. Click on the device icon or call path will open the snapshot page of the device or the call path respectively.

Accessing VoIP Monitor Business Views

1. Mouse-over **Maps** tab and select **VoIP Monitors**.
2. Click **Business Views**.
3. Select the required business view from the drop down menu available on the top the business view displayed.

Viewing Top 10 Call Paths

With VoIP Monitor you can view the top 10 call paths by MOS, Packet Loss, Jitter and Latency. This provides you to have a quick view and react proactively. To view the top 10 call paths, follow the steps given below:

1. Mouse-over **Maps** tab and click on **VoIP Monitors**.
2. Click on **Top 10**. The top 10 call paths by MOS, Packet Loss, Jitter and Latency are listed.
3. Click on the required call path view its snapshot page.

Viewing VoIP Monitor Alerts

Go to Maps-> VoIP Monitor-> Alerts to view the alerts raised by WAN Monitor. All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.

Viewing VoIP Monitor Reports

The VoIP Monitor reports help you to view the various metrics such as jitter, MOS, RTT etc. to determine the health of the VoIP networks. To generate the VoIP monitor reports, follow the steps given below:

1. Mouse-over **Maps** tab and select **VoIP Monitors**.
2. Click on **Reports**. The default **History reports** and **Top N reports** are listed.
3. Click on the required report.

You can also access the VoIP Monitor reports from Reports tab. The generated report can be emailed or exported to a PDF version by click the respective icons on the report.

FAQs on VoIP Monitor

1. Why do i need to set SNMP write community on the Source Router ?

Both, the SNMP read and write community string needs to be set on the source router. The write community is used to configure the IPSLA on the device while the read community is used by OpManager to gather performance data from the router. [back to top]

2. Why I am getting 'Source router SNMP write community may be wrong' error message?

OpManager uses SNMP to gather data from the Cisco IP SLA agent. This error is displayed when wrong SNMP read / write community string is configured for the Source router of the VoIP Monitor in OpManager.

To configure the correct SNMP write community string in OpManager, go to the snapshot page of the source router and change the SNMP credentials by clicking on the '**Click here to change**' corresponding to the "**Passwords**" field. In the pop-up enter the appropriate credentials and submit it. After successfully submitting the correct SNMP credentials, try to add the VoIP Monitor again for the Source device (Maps > VoIP Monitor > Settings). [back to top]

3. Why should the SLA Responder be enabled on the destination device ?

Enabling the IP SLAs Responder provides the details of packet loss statistics on the device sending IP SLAs operations. IP SLAs Responder is enabled on the target router (rtr responder) before configuring a Jitter operation. [back to top]

4. Why are the VoIP metrics shown as zero or 'Not available' in OpManager?

You will see zero or 'not available' values when data is not collected for the monitored metrics. This can be either due to incorrect SNMP read community configured, or of the Responder is not enabled on the destination device. Make sure that the correct SNMP read community is configured and the SLA Responder is enabled. [back to top]

5.What are the critical parameters monitored to determine the VoIP QoS performance?

The monitored parameters include Latency, Jitter, Packet Loss, and MOS. The parameters are described below for reference:

Jitter : Jitter is defined as a variation in the delay of received packets. Users often experience disturbing sounds over a conversation coupled with loss of synchronization at times and is referred to as jitter. High levels of jitter can result in some packets getting discarded and thereby impact the call quality. Ensuring a jitter-free transmission to provide qualitative service depends on identifying the bottle-neck responsible for the jitter, and acting on it to eliminate it. OpManager's VoIP monitoring feature helps you find the problem and ensures maximum QoS on your VoIP network.

Packet Loss : Packet loss is a measure of the data lost during transmission from one resource to another in a network. Packets are discarded often due to network latency. Using OpManager, you can monitor the packet loss and take corrective actions based on the information.

One way Latency: Latency (delay) is the time taken for a packet to reach the destination device. When monitoring latency over VoIP, the delay measured is the time taken for a caller's voice at the source site to reach the other caller at the destination site. Network latency contributes to delay in voice transmission, resulting in huge gaps between the conversation and interruptions.

Round Trip Time: Round Trip Time is the time taken for a packet to reach the destination and again comes back to the source device. The total time it takes for the round trip is measured in milliseconds.

MOS: The Mean Opinion Score is the key quality indicator of VoIP traffic quality. And is measured in the scale of 1 to 5 (poor to excellent quality). [back to top]

6. What is VoIP codec?

Codecs (Coder/Decoder) serve to encode voice/video data for transmission across IP networks. The compression capability of a codec facilitates saving network bandwidth and it is therefore appropriate that you choose the correct codec for your IP network. Here is a quick reference to the codecs with the corresponding packets size and bandwidth usage:

Codec & Bit Rate (Kbps)	Operation Frequency	Default number of packets	Voice Payload Size	Bandwidth MP or FRF.12 (Kbps)	Bandwidth w/cRTP MP or FRF.12 (Kbps)	Bandwidth Ethernet (Kbps)
G.711a/u (64 kbps)	60 msecs by default. You can specify in the range of 0 - 604800 msecs.	1000	160 + 12 RTP bytes	82.8 kbps	67.6	87.2
G.729 (8 kbps)		1000	20 + 12 RTP bytes	26.8 kbps	11.6	31.2

[back to top]

7. How much bandwidth does each monitor occupy ?

The bandwidth occupied depends on the codec selected. Look at the above table for reference. [back to top]

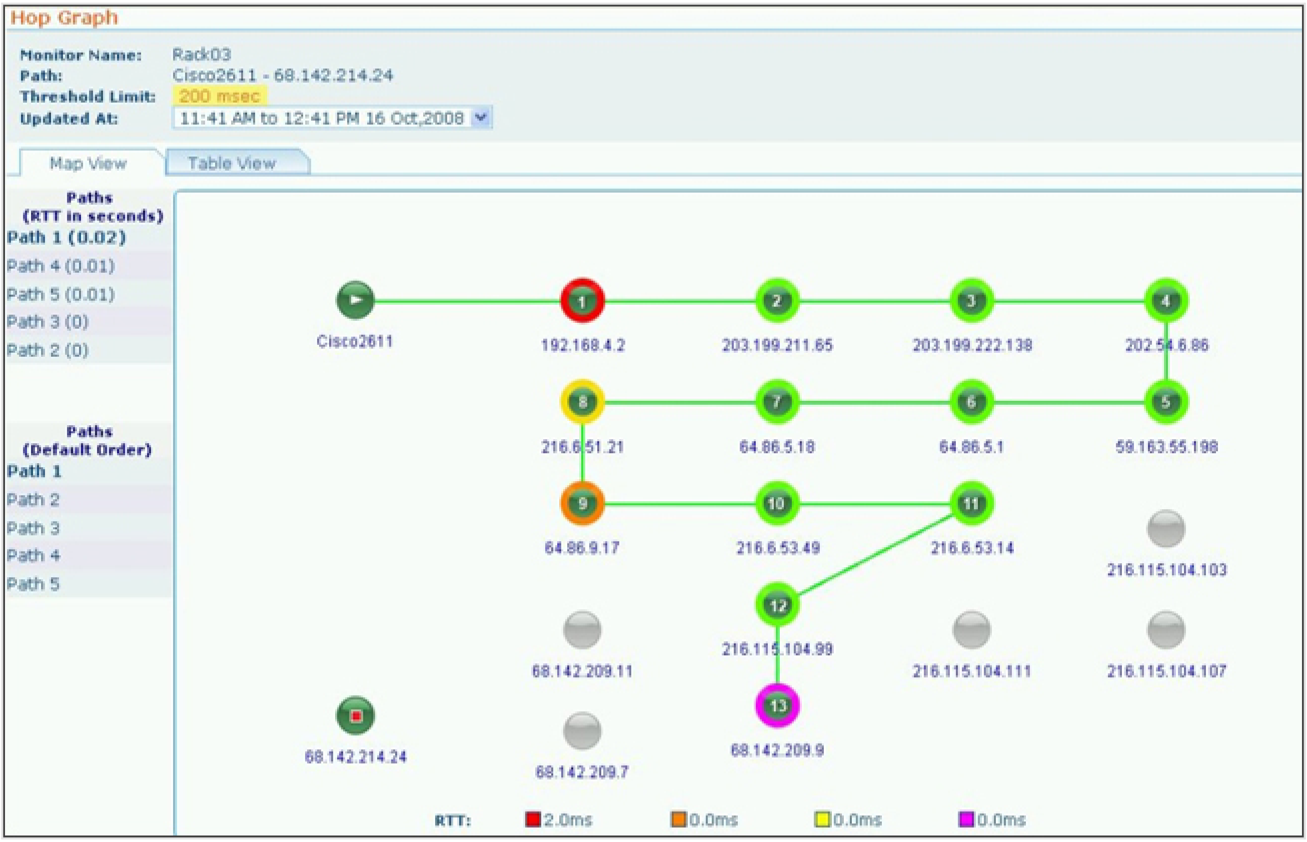
About WAN Monitor

The WAN monitoring feature in OpManager is an add-on feature and requires license to run. The WAN monitor monitors the availability of all your WAN links, the Round Trip Time (RT) / Latency and the traffic details. Alerts are triggered when the set thresholds are violated, enabling the administrators to attend to the fault in no time.

OpManager uses Cisco's IPSLA agent to monitor the health and performance of the WAN links, and the prerequisite therefore is, that the device must be a Cisco router (IOS version 12.3 or later) and it should have IPSLA agent enabled on it. Almost all the routers from Cisco are enabled with IPSLA agent and we support from IOS version 12.3 or later. The performance of the WAN link is measured by sending simulated traffic (packets of specified size) at a specified frequency. So the health of the WAN link / path is monitored round the clock . It helps the IT Engineer to proactively notice the problem. The Round Trip Time data is collected and persisted to measure the performance and also for reporting. Also, OpManager triggers alert when a Round Trip Time threshold is violated.

OpManager collects IPSLA traps for events triggered due to a connection loss or threshold violation for RT. When any such failure occurs, OpManager immediately triggers a Trace Route operation automatically to help the IT Engineer trace the fault to the exact hop. Further, the Trace Route report shows RT data for five different paths and 15 hops in a path. This enables you to troubleshoot and get to the root of the problem much quicker, resulting in very less downtime.

Besides this intelligent monitoring of the links across each hop, Netflow traffic reports also integrated in this new release. This enables you to identify any latency caused by the LAN traffic. You simply need to select all the WAN links / path to be monitored once and configure it. A sample trace route graph is given below:



Hop Graph

Monitor Name: Rack03
Path: Cisco2611 - 68.142.214.24
Threshold Limit: 200 msec
Updated At: 11:41 AM to 12:41 PM 16 Oct,2008

Paths (RTT in seconds)
Path 1 (0.02)
Path 4 (0.01)
Path 5 (0.01)
Path 3 (0)
Path 2 (0)

Paths (Default Order)
Path 1
Path 2
Path 3
Path 4
Path 5

RTT: 🟥2.0ms 🟧0.0ms 🟨0.0ms 🟪0.0ms

Configuring WAN Monitor

Prerequisites

OpManager primarily relies on Cisco's IP-SLA for monitoring the WAN and the prerequisite therefore is that the device should be a Cisco router and must have IPSLA agent enabled on it. Almost all the routers from Cisco were enabled with IPSLA agent and we support from IOS version 12.3 or later. OpManager uses SNMP to query the Cisco routers for the links' performance data. IPSLA familiarity is not a prerequisite. You just need to tell OpManager which links you want to monitor. OpManager provides an intuitive configuration wizard to help you configure all the IPSLA parameters for monitoring the WAN health.

Steps to set up the WAN Monitor

Using OpManager, you can now monitor the availability and latency of a WAN link / path. A WAN link mentioned here is the path between the router in your main office and the one in the branch office that you wish to monitor.

Step 1 : Add (/ discover) the router in your LAN to OpManager. And make sure the snmp read and write community are configured properly, for that router.

Step 2: Configuring the Router to send traps

Configure the cisco router to send traps to OpManager. Alerts are shown based on the traps received in OpManager. To configure OpManager server as the SNMP Server receiving traps for the routers, telnet the router and type the following command:

snmp-server host <opmanager server IP> traps <host community string> rtr

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:

```
snmp-server host 192.168.18.128 traps private rtr
```

Step 3: Creating the WAN Monitor

a. Go to the Maps tab (on from the list of Infrastructure views), click on-> WAN Monitors-> Settings
b. Select the source router from the list of routers discovered in OpManager and then select the relevant interface of the source router
c. Specify the destination Ip Address either by using the 'Search' option to pick from the discovered routers, or directly enter the IP Address and click 'Add' and submit the details.
d. You will see the summary of the monitor you are about to configure. Now click 'Apply to device' to submit the details to the device. This will take few seconds to configure.
Refresh the page after few seconds to see the new monitor. The data is collected every hour, from the time you have configured.

[or]

You can also create the WAN monitor from the Router snapshot page. To do so, go to Router snapshot page, click on Action tab and select Add WAN Monitor. Enter the Monitor Name and Destination IP. Click Submit to create the monitor or Click Advanced button to go to Create New WAN Monitor page and follow the steps from b to d given under Step 3.

To edit any of the configuration details, go to the respective template, make the changes and save the details. When you create a new monitor, the updated values take effect. When the configuration is complete, the router starts collecting the data at the specified frequency 60 seconds (default value). OpManager updates this statistics (collected data) every hour and the reports are generated after one hour of configuration.

Configuring Test Parameters and Threshold Template for WAN Monitor

Define a template with the required WAN monitoring settings to be used for monitoring performance. The RTT template comes with pre-populated default values. OpManager uses the configured values to simulate traffic. Incase you would like to effect some changes to the values before initiating monitoring, make the changes as follows

Configuring Test Parameters

OpManager uses the default settings specified here,

- **Payload**:The default value is 24 kb. Specify an echo payload value in the range of 0 to 16384.
- **Type of Service**: Specify the Echo TOS in the range of 0 to 255, the default being 30.
- **Operation Frequency**: Specify the interval in the range of 0 to 604800 msecs. The default interval is 60. The operation frequency is the frequency with which QoS metrics are collected by the IP SLA agent on your network to determine performance.
- **Operation Timeout**: Specify the timeout in the range of 0 to 604800000, the default being 60 msecs. Make sure that the timeout interval is lesser than the configured operation frequency so that if the operation is not successful, that is, if there is no response from the device, or in the event of a delay, the request is timed out and the subsequent operation is launched at the configured frequency correctly.

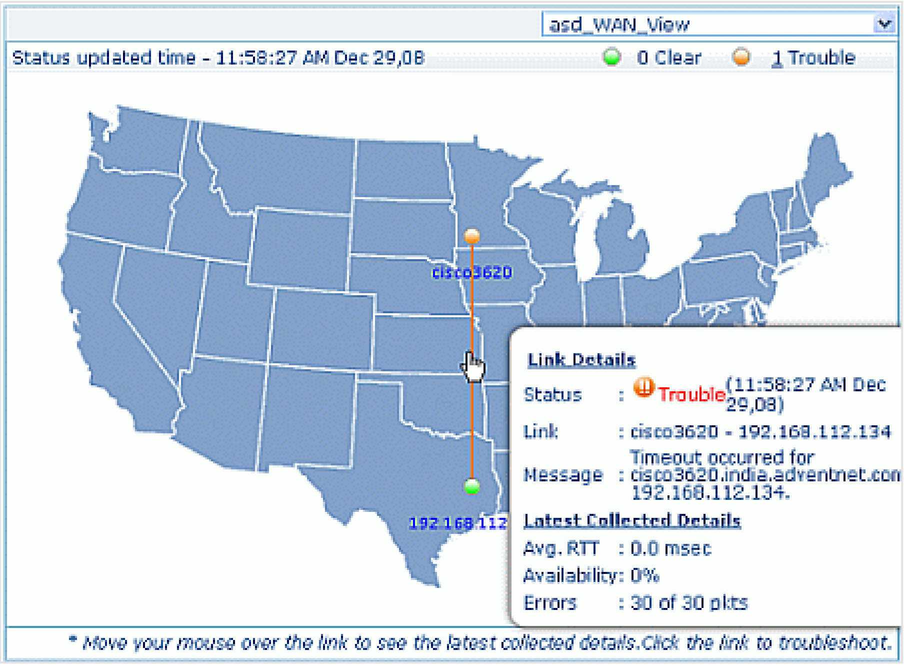
Defining Threshold for Round Trip Time

You can define a threshold template so that you are alerted with the WAN monitor violates a specified value. Here are the steps to define a threshold template:

1. Go to WAN Monitors > Settings page> Threshold Template.
2. Configure the upper and lower threshold limits for Round Trip time in msecs, the range being 0 to 60000 msecs. You can also choose various notification profiles configured in OpManager to alert you.

Business Views in WAN Monitor

In WAN Monitor, business views help you to know the status of the device and WAN link between devices at a glance. Whenever a new WAN monitor is created, a business view (image shown below) of it also gets created automatically with the default background and device icons. However, later you can modify the background and device icons if required.



Status updated time - 11:58:27 AM Dec 29,08 ● 0 Clear ● 1 Trouble

Link Details

Status : Trouble (11:58:27 AM Dec 29,08)

Link : cisco3620 - 192.168.112.134

Message : Timeout occurred for cisco3620.india.adventnet.com 192.168.112.134.

Latest Collected Details

Avg. RTT : 0.0 msec

Availability: 0%

Errors : 30 of 30 pkts

** Move your mouse over the link to see the latest collected details.Click the link to troubleshoot.*

In the business view, mouse-over the device icon or name/IP and WAN link to view its details. Clicking on the device icon will open the snapshot page of the device. Clicking on the WAN path opens the snapshot of the WAN path if it is in Clear state else opens the Hop graph in order to trace the fault to the exact hop.

Accessing WAN Monitor Business Views

1. Mouse-over **Maps** tab and select **WAN Monitors**.
2. Select the required business view from the drop down menu available on the top the business view displayed under the **Overview** tab.

Viewing WAN Monitor Alerts

Go to Maps-> WAN Monitor-> Alerts to view the alerts raised by WAN Monitor. All the alarms are listed with the Source name, Alarm Message, Status of the Device, Technician, Device category, date and time. Click the alarm message to view the alarm history.

Viewing WAN Monitor Reports

The WAN Monitor reports help you to view the reports on RTT threshold violation, RTT trend, Top N paths with Maximum RTT etc. to determine the health of the WAN links. To generate the WAN monitor reports, follow the steps given below:

1. Go to Reports-> WAN Monitor.
2. Click on the required report.

The generated report can be emailed or exported to a PDF version by click the respective icons on the report.

FAQs on WAN Monitor

1. Why there are no alerts from the device?

You might not have received alerts from the device if the trap host is not configured in the source Router. Make sure you configure the routers to send traps to OpManager. Telnet the router and type the following command:

snmp-server host <opmanager server IP> traps <host community string> rtr

For instance, if the OpManager host IP Address is 192.168.18.128, and the community string is private, the command would be:

snmp-server host 192.168.18.128 traps private rtr

2. Why should i give Snmp Write community to the router?

Both, the SNMP read and write community string needs to be set on the source router. The write community is used to configure the IPSLA agent on the device while the read community is used by OpManager to gather performance data from the router.

3. Why I am getting 'Source router SNMP write community may be wrong' error message?

OpManager uses SNMP to gather data from the Cisco IP SLA agent. This error is displayed when wrong SNMP read / write community string is configured for the Source router of the WAN Monitor in OpManager.

To configure the correct SNMP write community string in OpManager, go to the snapshot page of the source router and change the SNMP credentials by clicking on the '**Click here to change**' corresponding to the "**Passwords**" field. In the pop-up enter the appropriate credentials and submit it. After successfully submiting the correct SNMP credentials, try to add the WAN Monitor again for the Source device (Maps > WAN Monitor > Settings).

About NCM Plug-in

The Network Configuration Management (NCM) plug-in a complete solution for easily Network Change and configuration Management. It offers multi-vendor network device configuration, continuous monitoring of configuration changes, notifications on respective changes, detailed operation audit and trails, easy and safe recovery to trusted configurations, automation of configuration tasks and insightful reporting.

The NCM plug-in manages network devices such as switches, routers, firewalls, wireless access points, integrated access devices etc., from multiple vendors. It imports the network devices from OpManager, builds up an inventory database and allows IT administrators to take control of configuring the devices from a central console. The added advantage with the NCM plug-in is that no need to again configure users and mail servers, the configuration that are made in OpManager itself is sufficient.

Installation Platfrom:
NCM plug-in supports only Windows installations as of now.

Database:
NCM plug-in uses the same MySQL bundled with OpManager.

Ports Used:

- Syslog: 519
- Web: 6060
- TFTP: 69
- SSHD: 22
- MySQL: 13306

Features:

- Multi-vendor configuration for switches, routers, firewalls and other devices
- Real-time configuration tracking and change notification
- Effective Change Management Policies
- Quick restoration to trusted configurations through a few simple steps
- Templates for commonly used configurations
- Automation of important device configuration tasks
- Encrypted storage of device configuration in database
- Contextual, side-by-side comparison of altered configuration
- Examining device configurations for compliance to a defined set of criteria/rules
- Comprehensive Audit Trails
- Detailed reports on inventory and configuration changes

Note:
Support for LDAP, RADIUS & Active Directory are disabled in this plug-in.

Installing NCM Plug-in

Download the NCM plug-in from OpManager website and follow the procedure given below to install:

1. Download OpManager's NCM plug-in file to OpManager server.
2. Shutdown OpManager Service.
3. Double click OpManager's NCM plug-in exe file. (You have to install NCM plug-in in OpManager server only)
4. Follow the on-screen instructions to complete the installation process.
5. Start the OpManager Service.

Note: You should have OpManager 8000 build or later.

Configuring MySQL Server

NCM plug-in uses the same MySQL bundled with OpManager. However, if you are running any other MySQL (other than OpManager's) on the port 13306, NCM plug-in fails to connect to that MySQL and therefore the NCM server (DeviceExpert server) does not start up. If you wish to use the MySQL other than OpManager's running on the port 13306, follow the below procedures:

1. In <DeviceExpert_Home>/conf/Persistence/persistence-configurations.xml, change the value for the configuration parameter "StartDBServer" to 'false' as shown below: (default value 'true')

   <configuration name="StartDBServer"value="**false**"/>
2. Also in your MySQL, creat a database with the name "deviceexpert".

   Use the following command to create the database

   mysqladmin -u root -P 13306 create <databasename>

   (Here, 13306 denotes the MySQL port in DeviceExpert)

Importing Devices into NCM Module

Pre-requisite

The pre-requisite to import devices to DeviceExpert is that the devices must be discovered in OpManager.

Importing Devices to DeviceExpert

To import the devices to DeviceExpert follow the steps given below:

1. From OpManager, click on the Network Configuration Management link available in the header. Or From DeviceExpert, click Inventory tab. The inventory page opens
2. Click on Import tab and select Import devices, if the device is SNMP enabled or click on Import SNMP devices.

Use the **Import SNMP Device** option to import the devices that are SNMP enabled (except Desktops) as DeviceExpert itself takes care of everything right from configuring the Device category to identifying the serial and model numbers. Whereas, you can use **Import Device** option to import the Desktops that are SNMP enabled and other devices that are not SNMP enabled. In this case you need to manually enter the serial and model numbers.

Import Device:

1. Select the Host Name/IP Address, Vendor and Device Template Name of the device that is to be imported.
2. Specify its Serial and Model numbers.
3. Click Add.

Import SNMP Device:

1. Select the devices that are to be imported from the left column and move to the right column.
2. Click Import.

The devices are imported into DeviceExpert.

Configuring NCM Module

Having installed and setup the NCM module, you will need to configure the module for network configuration management.

Following is a link to the detailed documentation for NCM module. Refer to the sections starting from 'Providing Credentials'.

Configuring NCM (DeviceExpert)

About NetFlow Plug-in

The NetFlow Analyzer plug-in offers a complete solution to perform in-depth traffic analysis on your network. NetFlow Analyzer uses the flows (netflow, sflow, jflow etc.) exported by the devices to identify traffic caused by them. NetFlow Analyzer provides you the detailed information on the bandwidth being used by the network and allows you to drill down to specific application, conversation, port, user etc that is consuming more and causing the damage. Futher you can generate detailed reports on the bandwidth patterns and take some capacity planning decisions.

By plugging in NetFlow Analyzer with OpManager you can view the traffic handled by the interfaces in their respective snapshot pages. The added advantage with NetFlow Analyzer plug-in is, the user defined in OpManager can access NetFlow Analyzer. Configuring mail server settings in NetFlow Analyzer is also not necessary if it has been configured in OpManager.

The devices that are NetFlow Analyzer enabled are marked with the NetFlow Analyzer icon in their respective maps. The interfaces that are NetFlow enabled are displayed with the icon under the Interface tab in their respective device snapshot pages.

Installation Platform:
NetFlow Analyzer plug-in supports only Windows installation as of now.

Supported DB:
NetFlow Analyzer pug-in supports only MySQL.

Devices Supported:
Click here to get the list of devices that are supported by NetFlow Analyzer.

Ports Used:

- Web: 8080
- NetFlow Listener Port: 9996
- MySQL: 13306

Features:

- Easy Network Troubleshooting
- NetFlow Reporting
- Network Security
- Application Performance Optimization
- Network Traffic Analysis
- Bandwidth Reporting
- Automating Reports
- Faster Network Troubleshooting
- Department wise bandwidth monitoring

Note: Radius Server is not supported in this NetFlow Analyzer plug-in.

Installing NFA Plug-in

Click here to download the NetFlow Analyzer plug-in. Follow the procedures given below to install:

1. Download OpManager's NetFlow Analyzer plug-in file to OpManager server.
2. Shutdown OpManager Service.
3. Double click OpManager's NetFlow Analyzer plug-in exe file. (You have to install NetFlow Analyzer plug-in in OpManager server only)
4. Follow the on-screen instructions to complete the installation process.
5. Start the OpManager Service.

Note: You should have OpManager 7205 build or later.

Configuring NFA Module

Having installed and setup the NFA module, you will need to configure the module for bandwidth and network traffic analysis. Following is a link to the detailed documentation for NFA module. Refer to the sections starting from 'Configuring Flow Exports'.

Configuring NFA (NetFlow Analyzer) Module

IP Address Management (IPAM) Plug-in

IPAM plug-in helps you identify whether an IP Address is currently available or not, in an enterprise network. The IPAM plug-in periodically scans a subnet and provides the availability status of IP addresses in that subnet. This helps you identify whether a particular IP is reserved or available. The plug-in accepts multiple subnet inputs, which helps in scanning the entire network to get the status of the IP Addresses.

The IPAM plug-in also includes Switch Port Mapper that helps you identify the switch port to which a device is connected and thus eliminates the need of manually tracing the network cables. The switch port mapper discovers the devices plugged into each port of a specified switch. This gives you the visibility into the IP, MAC, VLAN, status and availability of ports. Since this is a real-time discovery, you can also view the operational status and speed of each port.

OpManager - IPAM Plug-in Video:

Installing IPAM plug-in

Check our installation guide to know the steps to install IPAM plug-in.

Using IPAM Plug-in

Click here to access the IPAM plug-in user guide.

Applications Monitoring Plug-in

ManageEngine Applications Monitoring Plug-in is a comprehensive application monitoring software that helps businesses keep track over the performance of critical applications and thereby ensuring high availability. It helps monitoring the performance of various components of an application and provides quick resolution in case of any outages. This improves the quality of service to end-users.

Applications Monitoring plug-in offers out-of-the-box monitoring support for 50+ applications such as such Oracle, SAP, Sharepoint, Websphere and much more.

OpManager - Applications Monitoring Plug-in Video:

Installing Applications Monitoring plug-in

Check our installation guide to know the steps to install Applications Monitoring plug-in.

Using Applications Monitoring Plug-in

Click here to access the Applications Monitoring plug-in user guide.

Integrating with NetFlow Analyzer

OpManager can seamlessly integrate with the network traffic monitoring tool, Netflow Analyzer, one of the AdventNet ManageEngine suite of products. Netflow Analyzer provides detailed interface traffic reports.

To view the detailed traffic report from Netflow Analyzer, the prerequisites are,

1. Netflow Analyzer must be up and running in your network
2. The interface whose traffic you would like to monitor must be discovered in both, OpManager and Netflow Analyzer.
3. The NetFlow Analyzer settings must be configured properly in OpManager

Configure NetFlow Analyzer Settings

To configure the NetFlow Analyzer Settings in OpManager

1. Click **Admin** tab, click **Add-On/Products Settings**
2. Click **NetFlow Settings** icon in this screen
3. Type the following NetFlow Analyzer server details:
    1. Server Name
    2. Port (default is 8080)
    3. User Name
    4. Password
    5. Polling Interval in mins
4. Save the settings.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the Routers map
2. Click the required interface icon in the Routers map to see its snapshot page
3. In the Interface Traffic details column, do a mouse-over the **Netflow** icon. Select
    1. Top Applications
    2. Top Sources
    3. Top Destinations
    4. Top Conversations

Traffic details are shown in detail based on the above options.

Integrating with ServiceDesk Plus

If you have ServiceDesk Plus installed in your network, you can automatically log trouble tickets from OpManager for specific network faults. So, besides the provision to email, sms, or notify fault in other forms, you can also track the faults by logging trouble tickets to ServiceDesk Plus. This helps in issue tracking.

For logging the trouble ticket to ServiceDesk Plus correctly, you need to ensure the following:

1. Incoming Mail Settings must be configured properly in ServiceDesk Plus
2. ServiceDesk Plus Settings must be configured in OpManager
3. A notification profile to log a trouble ticket to ServiceDesk Plus must be configured and associated.

Configure Servers Settings

Following are the steps to configure the ServiceDesk Plus and OpManager Server settings:

1. Configure Incoming Mail Settings in ServiceDesk Plus
2. Configure Mail Server Settings in OpManager
3. OpManager must 'know' where ServiceDesk Plus resides to log the ticket. To configure the ServiceDesk Plus settings details, follow the steps given below
4. Click **Admin** tab, and select **Add-On/Products Settings** and configure the following values:

   Server where ServiceDesk Plus is running: Name or the IP address of the machine where ServiceDesk Plus is installed and running.

   ServiceDesk Plus server port number : The port number in which the ServiceDesk Plus application is running. Default port is 8080.

   ServiceDesk Plus login: The user name with which you will log in into ServiceDesk Plus. Default is **admin**

   ServiceDesk Plus password : The password to log in into ServiceDesk Plus. Default password for **admin** user is **admin**

   HelpDesk Email Address : The email address in the mail server to which the email must be sent. This should be the same as configured in the mail-server settings in ServiceDesk Plus. Example: help@servicedeskplus.com

   From Email Address : The initiator's email address. Example: requestor@company.com

Integrating with DeviceExpert

OpManager can seamlessly integrate with the DeviceExpert, a network change and configuration management solution for network devices. The configurations of devices like routers, switches, and firewalls can be managed using this solution. When integrating with OpManager, you can monitor the devices and their resources for performance, and also manage changes and configurations across these devices.

To view the configuration and the changes from OpManager,

1. DeviceExpert must be up and running in your network
2. The network devices whose changes you want to monitor must be discovered in both, OpManager and DeviceExpert.
3. The DeviceExpert settings must be configured properly in OpManager

Configure DeviceExpert Settings

To configure the DeviceExpert Settings in OpManager

1. Copy the file server.keystore from /DeviceExpert/conf folder to a folder on your local machine.
2. From OpManager WebClient, select **Admin** tab and click on **Add-On/Products Settings**
3. Click **DeviceExpert Settings** link in this screen
4. Type the following DeviceExpert server details:
    1. Server Name
    2. Port (default is 6060)
    3. Browse and select the server.keystore file copied to the local machine.
    4. User Name
    5. Password
    6. Hit **Test Connection and Save** option to verify the integration.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the snapshot page of the Router/Switch/Firewall
2. From the **Device Info** menu, select **Startup Configuration** to see the initial configuration of the device.
3. From the same menu, select **Running Configuration** to see the runtime configuration changes made to the device.

Troubleshooting

What to do when you encounter an error message 'Unable to fetch values from DeviceExpert, The server might not be running or the network traffic may be too high' when configuring the DeviceExpert details in OpManager:

- Check if the DeviceExpert service details are correctly configured. Specially, the port number and the proper server.keystore file is selected.
- Despite correct details, if you still face issues, try the following:
    - Open a command prompt and change directory to /opmanager/bin
    - Execute the script ssl_deviceexpert.bat with the absolute path of OpManager installation folder. For instance, if the OpManager path is C:Program FilesAdventNetMEOpManager, the script should be executed as follows:

      C:Program FilesAdventNet1MEOpManagerbin>ssl_deviceexpert.bat "C:Program FilesAdventNet1MEOpManager"

Integrating with Firewall Analyzer

OpManager can seamlessly integrate with Firewall Analyzer, a web-based Firewall Log Analysis & Reporting Tool. Integrating OpManager with Firewall Analyzer allows you to monitor your Server's Security, Traffic, & Bandwidth utilization in depth.
To view the detail traffic and security reports from Firewall Analyzer, the prerequisites are,

1. Firewall Analyzer must be up and running in your network
2. The firewall whose logs you would like to analyze must be available in both, OpManager and Firewall Analyzer. That is, configure your firewalls to forward syslog messages to the server running Firewall Analyzer. These firewalls should be discovered in OpManager for monitoring.
3. The Firewall Analyzer settings must be configured properly in OpManager.

Configure Firewall Analyzer Settings

To configure the Firewall Analyzer Settings in OpManager

1. Click **Admin** tab, click **Add-On/Products Settings**
2. Click **Firewall Analyzer Settings** icon in this screen
3. Type the following Firewall Analyzer server details:
    1. Server Name
    2. Port (default is 8500)
    3. User Name
    4. Password
    5. Select the Polling Interval in minutes
4. Test and save the settings by clicking on **Test Connection and Save** button.

After configuring the settings, you can follow the steps given below to see the detailed reports:

1. Go to the Firewalls map
2. Click the required Firewall icon in this map to see its snapshot page
3. From the **Reports** menu on the right in the snapshot page, select any of the following options to view the respective reports:
    1. Traffic Reports
    2. Security Reports
    3. Custom Reports
    4. All Reports

Detailed reports retrieved from Firewall Analyzer are shown based on the reports selected.

Integrating with ITPulse

About ITPulse

ITPulse is a private social network built exclusively for IT. With ITPulse, you can start discussions, and share articles and videos.

Benefits of this integration:

Any alarm that a technician acknowledges, unacknowledges, or clears, it is automatically posted on ITPulse wall. Other IT team members can know the status and can also discuss on the alarm or view its details from ITPulse itself, by clicking on the alarm link.

Configure ITPulse settings

Prerequiste: Create a login for the user in ITPulse

1. Mouseover Admin link available on the top right corner and select Map ITPulse Account
2. Enter the email ID address and password.
3. Click Save button.

That's it you have mapped the user's OpManager and ITPulse accounts. It has to be done similarly for every other user in OpManager.

How to video:

Rebranding OpManager

Rebranding option helps you replace OpManager logo that is displayed in the OpManager web client as well as in the reports, with your company's logo. You can also change the product name, company name and copyright details.

To replace OpManager's logo with your Company's logo in the OpManager web client and reports, follow the steps given below

1. From Admin tab, click Rebrand OpManager under Tools.
2. Click the change link Header Image and Report Header Image to replace the OpManager logo that is displayed in OpManager web client and reports.
3. Browse your logo and import.

To replace the product name, company name and copyright follow the steps given below:

1. Enter the Company Name and Product Name that you want to display in the Reports.
2. Enter the Copyright Text.
3. Click Submit.

Once done with the above changes, restart OpManager.

Configuring Database Maintenance

To plot graphs and generate reports, OpManager collects data from the managed devices at regular intervals. By default, OpManager aggregates the performance data into hourly data at the end of each hour. The hourly data thus calculated will be aggregated into daily data at the end of each day. These aggregated data will be used in graphs and reports.

OpManager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 7 days, the hourly data for 30 days and the daily data for 365 days. After the specified period, the database will be cleaned up automatically.

To configure your own settings for database maintenance, follow the steps given below:

1. Click the **Admin** tab.
2. Under **Tools**, click **Database Maintenance**.
3. Specify the values for the following fields:
    1. **Alarms Database**- the maximum number of recent alarms to be maintained must be specified here. For instance, if you want an history of last 500 alarms, specify the value as 500 here.
    2. **Events Database**- multiple events correlate to generate a single alarm. This is essentially a history information.
    3. **Performance Database**- the cleanup interval of the raw data as well as the archived data must be specified here.
4. Click **OK** to apply the changes.

Scheduling Downtime

Maintenance of network devices forms an integral part of network administration. You may want to perform a maintenance of specific device types at specific intervals. If such devices are removed from the network, or rebooted, then you will see alarms indicating that the device, or the applications in the device are unavailable. Since the devices are not available when polled for status during the maintenance period, unnecessary alarms are fired. To prevent the devices from being monitored for status during maintenance, you can schedule a maintenance task for such devices.
Following are the steps:

1. From the **Admin** tab, select **Downtime Scheduler** option under **Tools**.
2. Click on **New Schedule**.
3. In the **New Downtime Schedule** form, provide the following details:
   - Schedule Name
   - Schedule Description
   - Select the Status as **Enabled**, if you want the Scheduled task to take effect immediately. Else select **Disabled**, so that you can enable it when required.
   - Select the frequency at which the Task has to be scheduled/executed. It can be **Once**, **Every Day**, **Every Week,** and **Every Month**.
   - Specify the start and end time/day of the task in the corresponding fields.
   - If it is a schedule to be executed **every day**, then specify the date from which the task must be scheduled.
   - If it is a monthly schedule, select either the date or the day with the time window for the schedule.
   - You can assign the task to only the required devices, or a device category like switches, routers, to a Business view, or to URL Monitors.

The schedule will be executed as configured.

Scheduling Reports

OpManager allows you schedule a new report and also to schedule a generated report.

Schedule a new report

1. From Admin tab, select **Select Schedule Reports** under **Tools**.
2. In the Report Scheduler page, click the **Add Schedule** button on the right.
3. Configure the following details:
    1. **Name**: Configure a name for the schedule.
    2. **Choose Report Type**: All the available reports types can be scheduled.
    3. Click **Next**.

Scheduling Top N Reports / All Devices reports:

If you have selected to schedule the Top N Reports, configure the following details:

1. **Top N Reports**: Select from Top 10/25/50/100 reports.
2. **Period**: Choose the period for which you want the report scheduled.
3. **Select Report(s)**: Select the required resource reports to be scheduled.
4. **Business View Reports**: Select the relevant check-box and the business view to generate reports specific to the devices in that business view.
5. Click **Next**.

Scheduling Device specific Availability reports:

If you have chosen to schedule reports for device specific availability details, configure the following:

1. Select either a category of devices, or the required business view, or select specific devices manually for generating the availability reports.
2. Select the period for which you want to generate the reports.
3. Click **Next**.

Configuring the Time Settings for generating reports:

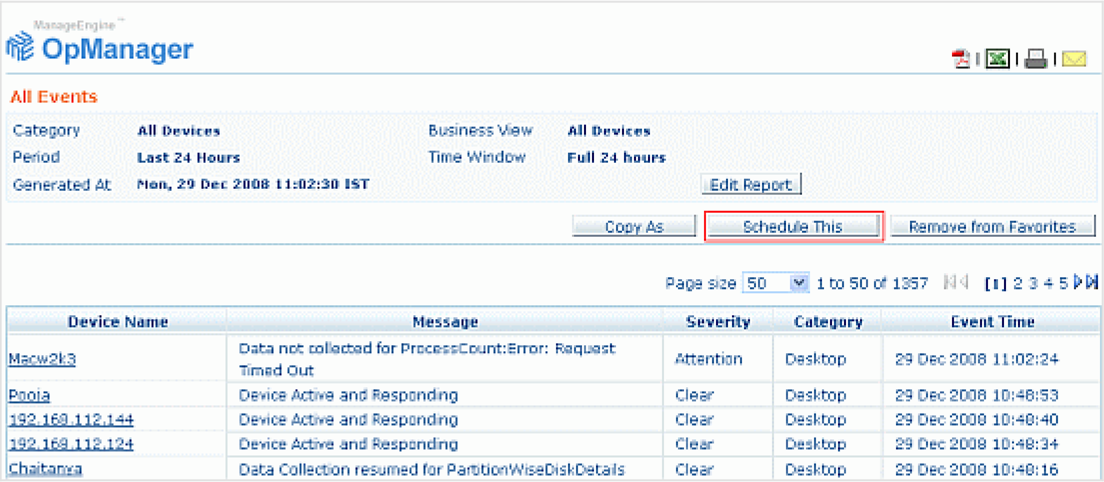
1. **Daily**: Select the time at which the reports must be generated every day.
2. **Weekly**: Select the time and also the days on which the reports must be generated.
3. **Monthly**: Select the time, day, and the months for which the reports must be generated.
4. **Report Format Type**: Select either PDF or XLS to receive the report in the respective formats.
5. **Report Delivery**: Select any one of the following options.

- Configure the email ids to which the reports are to be sent as attachments. [or]
- Configure the url where the reports can be published.
- **Period**: Choose the period for which you want the report scheduled.
- **Select Report(s)**: Select the required resource reports to be scheduled.
- Click **Next**.

Verify the details of the configured schedule and hit **Submit** for the schedule to take effect.

Scheduling a generated report

1. In the report page that is generated, click **Schedule This** button to schedule the report.



All Events

Category	All Devices	Business View	All Devices
Period	Last 24 Hours	Time Window	Full 24 hours
Generated At	Mon, 29 Dec 2008 11:02:30 IST		

Page size 50 1 to 50 of 1357 [1] 2 3 4 5

Device Name	Message	Severity	Category	Event Time
Macw2k3	Data not collected for ProcessCount:Error: Request Timed Out	Attention	Desktop	29 Dec 2008 11:02:24
Pooja	Device Active and Responding	Clear	Desktop	29 Dec 2008 10:48:53
192.168.112.144	Device Active and Responding	Clear	Desktop	29 Dec 2008 10:48:40
192.168.112.124	Device Active and Responding	Clear	Desktop	29 Dec 2008 10:48:34
Chaitanya	Data Collection resumed for PartitionWiseDiskDetails	Clear	Desktop	29 Dec 2008 10:48:16

2. Enter the report name.
3. Select the time and period.
4. Enter the email ID to which the report has to be delivered.
5. Click **OK**.

Enabling the Configured Schedule

Once you configure the report schedules, they are listed in the Report Schedule page (Admin --> Schedule Reports page). Select the required schedules and click on the **Enable** button at the bottom of the list. You can also disable or delete a schedule from here.

Using the Quick Configuration Wizard

OpManager's quick configuration wizard helps you to configure monitors, notification profiles, dependency, and so on, for many devices at a time.

To invoke the wizard, in the **Admin** tab under **Configuration**, click **Quick Configuration wizard**.

You can perform the following configurations for multiple devices:

- Assign a notification profile to several devices
- Delete associated notification profile
- Add a new service monitor to several devices
- Add a windows service monitor to several devices.
- Associate Event log rules to several devices
- Configure Device Dependencies
- Associate a credential to several devices
- Delete devices
- Manage / Unmanage devices

MIB Browser: Overview

The MIB Browser tool is a complete SNMP MIB Browser that enables loading and browsing MIBs and allows you to perform all SNMP-related operations. You can also view and operate on the data available through the SNMP agent running on a managed device.

The features of MIB Browser include the following:

- Saving the MIB Browser settings.
- Loading and viewing MIB modules in a MIB tree.
- Traversing the MIB tree to view the definitions of each node for a particular object defined in the MIB.
- Performing the basic SNMP operations, such as GET, GETNEXT, GETBULK, and SET.
- Support for multi-varbind requests. This feature is available only in the Java client.
- Real-time plotting of SNMP data in a graph. Line graph and bar graph are the two types of graphs that are currently supported. This feature is available only in the Java client.
- Table-view of SNMP data. This feature is available only in the Java client.
- Enables loading of MIBs at startup. This feature is available only in the Java client.

MIB Browser Interface

- **Menu bar**: Contains menus with related commands to perform all administrative operations.
- **Toolbar**: Contains frequently used administrative commands for easy access.
- **MIB Tree**: Shows all the loaded MIBs. You can traverse the tree and view the definition of each node in the tree.
- **SNMP Settings**: Displays the SNMP settings of the selected node.
- **Result Display Area**: Displays the result of the SNMP operations.
- **Object Attributes**: Shows the attributes of the selected node

Switch Port Mapper

OpManager shows the connectivity between a switch and other connected devices in the network in Switch Port Mapper. You get the details such as the MAC address, IP Address and DNS names of the devices connected to the switch.

You need to provide the details such as the community string and port number of the switch and if needed, the details of the server or router that may contain the layer 3 details.

To view the switch port mapping details, follow the steps given below:

1. Click the switch icon in the map.
2. In the displayed Snapshot page, click **Switch Port Mapper** under **Device Info**.
3. Click **Show Mapping** in the Switch Port Mapper window to view the mapping details.

About Reports

Intuitive dashboards and detailed reports helps you determine the performance of your network in very less time. OpManager allows you to export the default reports to other file formats such as exporting to PDF or XLS. You can also schedule the reports to be emailed or published. The default reports available in OpManager include:

- **System**: Provides a complete report on all the system related activities of all the devices. This category of reports include All Events, All Down Events, SNMP Trap Log, Windows Event Log, Performance Monitor Log, Notification Profiles Triggered, Downtime Scheduler Log, Schedule Reports Log, All Alerts and All Down Alerts.
- **Health and Performance**: Gives you a detailed report on the health and performance of all/top N devices.
- **Availability and Response**: Gives you a detailed report on the availability and the response time of all/top N devices
- **Inventory**: Inventory reports are available for servers, desktops, all devices, SNMP-enabled devices and non-SNMP devices.
- **WAN Monitors**: Gives you a detailed report on RTT threshold violation, RTT trend, link availability and error statistics and Top N paths with Maximum threshold violation and RTT. (Also can be accessed from Maps-> WAN Monitors-> Reports)
- **VoIP Monitors**: Gives you a detailed report on the Jitter, MOS, RTT etc. history and top N call paths by Jitter, MOS, Packet loss and Latency. (Also can be accessed from Maps-> VoIP Monitors-> Reports)
- **My Favorites**: OpManager provides the option to categorize all your important and frequently viewed reports as you favorites.

Note: Exporting WAN Monitor and VoIP Monitor reports to XLS format is not supported at present.

Viewing Device Health Report at a Glance

Performance of various resources on a device can impact the health of that device. For instance, it can be due to insufficient hardware, high resource utilization of a resource by a process, too many processes running on that system, or too much incoming and out-going traffic, or even network latency.

OpManager helps you see the performance of all the resources at a glance for a single device. This helps troubleshooting the problem much easier.

To access this report, go to the device snapshot page and click on **At a Glance Report** option on the right corner. This is a report showing the device health at a glance. It shows details like the availability, response time, packet loss, resource utilizations etc.

Viewing Interface Reports

Interface reports help you to determine the health of the interface by generating detailed reports on In and Out Traffic, In and Out Errors and Discards, Bandwidth & Outage Report, At-a-Glance Report etc. The reports can be exported to PDF format, taken printouts or emailed by clicking the respective icons. To generate the interface reports, follow the steps given below:

1. Go to the snapshot page of the interface whose health report you want to generate.
2. Click on **Reports** tab available on the top right of the page. All the default reports that can be generated are listed.
3. Click on the name of the required report to generate current day's report. Click on the 7 or 30 days icon to generate the report for the last 7 or 30 days respectively.

Business View-based Reports

OpManager provides an intuitive Availability Dashboard for your business view. You can track the fault to the root in no time.

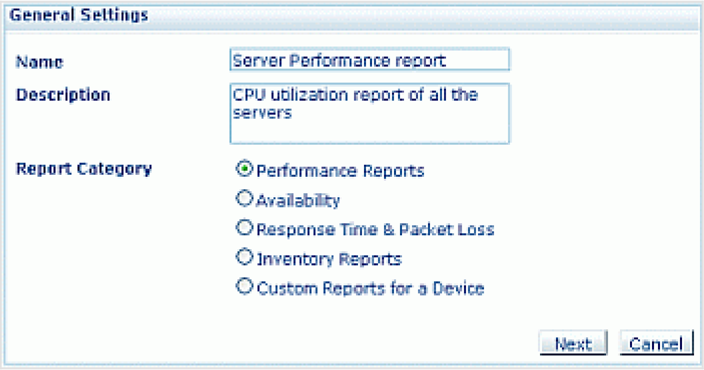
To access the business view dashboard, follow the steps below:

1. Go to the required business view.
2. Click on the **Dashboard** tab. The business view dashboard shows the availability distribution and also the least available devices in that view.
3. Click on the bar indicating a problem to drill down to the actual fault.
4. You can also view the dashboard for various periods like the last 24 hours, or last few days to analyze the trend.

Creating New Reports

Custom Reports option is replaced with Create New Reports option. The big advantage with Create New Reports option is that you can create your own reports, save them and generate whenever required. To create a new report follow the steps given below:

1. Click the **Create New Report** button under the Reports tab. Create New Report window opens.



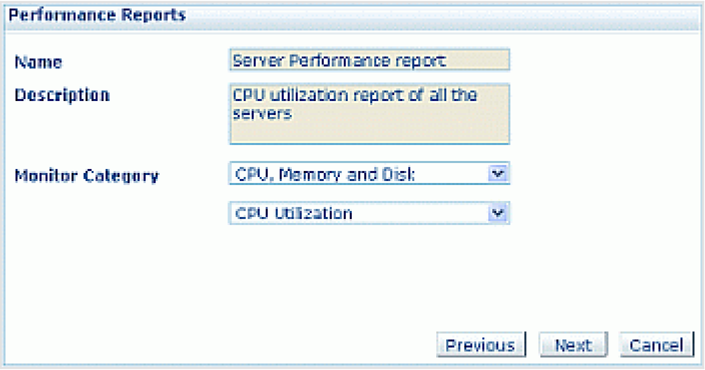
General Settings

Name: Server Performance report

Description: CPU utilization report of all the servers

Report Category:
● Performance Reports
○ Availability
○ Response Time & Packet Loss
○ Inventory Reports
○ Custom Reports for a Device

2. Enter a unique **Name** and brief **Description**.
3. Select the required **Report Category**. For instance, the report category is selected as Performance Reports.
4. Click **Next**.



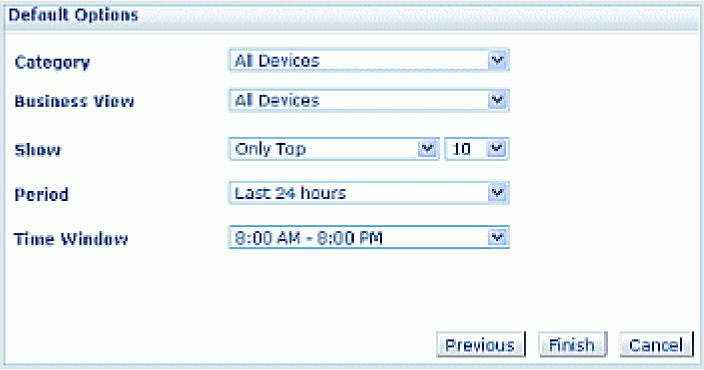
Performance Reports

Name: Server Performance report

Description: CPU utilization report of all the servers

Monitor Category: CPU, Memory and Disk
CPU Utilization

5. Select the **Monitor category**.
6. Select the sub category.
7. Click **Next**.



Default Options

Category: All Devices

Business View: All Devices

Show: Only Top 10

Period: Last 24 hours

Time Window: 8:00 AM - 8:00 PM

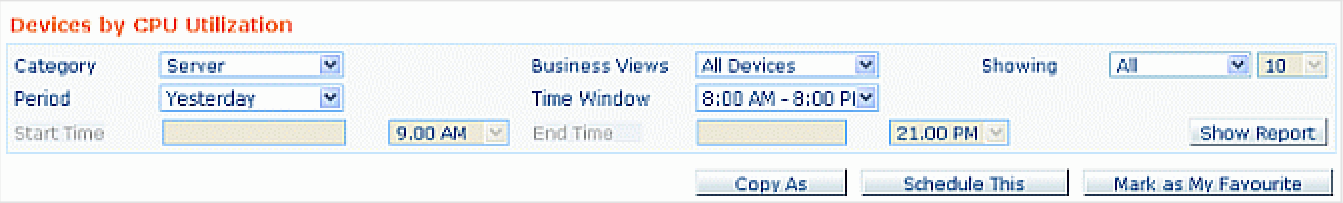
8. Select the required **Category**, **Business Views**, **Top N devices**, **Period** and **Time Window**.
9. Click **Finish** to create the new report.

The created report gets saved under the appropriate report category. Go to that category and click on the report to generate the report.

Editing Reports

OpManager allows you to edit a generated report in order to refine for some specific parameters, devices or time periods. To edit a generated report follow the steps given below:

1. Click **Edit** report button available on the top right of the report page.
2. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Top N devices.



Devices by CPU Utilization

Category: Server

Period: Yesterday

Start Time: 9.00 AM

Business Views: All Devices

Time Window: 8:00 AM - 8:00 PI

End Time: 21.00 PM

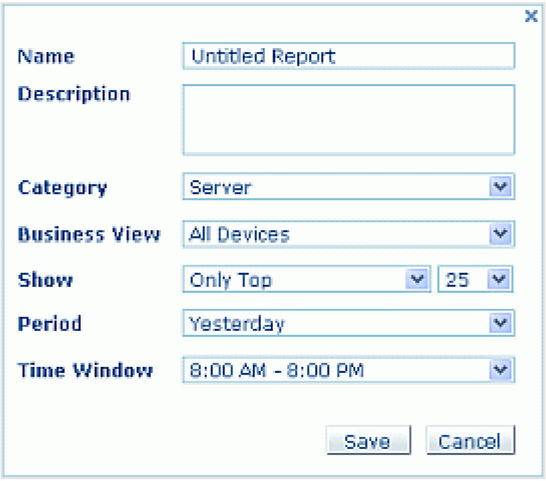
Showing: All 10

3. After modifying the required fields, click on **Show Report** to generate the report effecting the changes made.

Copying Reports

OpManager allows you to copy a generated report in order to retain the already configured parameters as template and do some minor changes on them and save as a new report. To copy and save a report follow the steps given below:

1. Click **Copy As** button available on the top middle of the report that is generated. A small window opens.



Name	Untitled Report
Description	
Category	Server
Business View	All Devices
Show	Only Top 25
Period	Yesterday
Time Window	8:00 AM - 8:00 PM

2. Enter a unique **Name** and a brief **Description**.
3. Change the required fields. The various fields that can be altered are Category, Period, Business Views, Time Window and Top N devices.
4. After modifying the required fields, click **Save** button to save the new report.

Configuring Favorite Reports

With OpManager you can mark the reports that are frequently viewed as Favorite reports. The reports that are marked as favorite reports are listed under My Favorites report category. To mark a report as your favorite one, follow the steps given below:

1. Generate the report that you want to mark as your favorite.
2. Click **Mark as My Favorite** button available on the top right of the report.

A message is displayed saying that "This report has been marked as your favorite".

Deleting a report from the Reports

To delete a report from your favorites list, follow the steps given below:

1. Go to **Reports**-> **My Favorites**.
2. Click the respective delete icon ✕ of the report that you want to remove from your favorites list. A confirmation dialog box opens.
3. Click **OK** to confirm deleting.

Note: Default reports available under My Favorites category cannot be deleted.

[or]

1. Generate the report that you want to remove from your favorites list.
2. Click **Remove from Favorites** button available on the top right of the report.

A message is displayed saying that " This report has been removed from your favorites list".

Time Based Availability Reports

You can generate time based availability reports of the devices from Reports-> Default reports-> Detailed reports. In the report page that is generated select the desired time name form the Time Window box available under **Report Options** in order to generate the report for that particular time period alone. You can add/modify/delete a time name from the Time Window box.

To add/modify/delete a time name open the Report Config file (OpManagerConf) with Notepad/word pad.

Add Time Name:
Enter a new time window name as given below in the Report Config file.

```
<Root>

    <Configurations>

        <TimeWindow Name="Full 24 hours" Value="0-24"/>

        <TimeWindow Name="8:00 AM - 8:00 PM" Value="8-20" />

        <TimeWindow Name="6:00 AM - 9:00 PM" Value="6-21" /> [New Time Window Name. Enter your desired values.]

    </Configurations>

</Root>
```

Modify Time Name:
Modify the existing time window name as given below in the Report Config file.

```
<Root>

    <Configurations>

        <TimeWindow Name="Full 24 hours" Value="0-24"/>

        <TimeWindow Name="10:00 AM - 10:00 PM" Value="10-22" /> [Existing Time Window Name that is modified. Enter your desired values.]

    </Configurations>

</Root>
```

Delete Time Name:
To delete an existing time window name simply delete that time window name in the Report Config file.
Note: After adding/modifying/deleting a time name restart the OpManager.

OpManager REST API

OpManager offers REST APIs for adding and fetching data from OpManager. Using these APIs, you can integrate OpManager with 3rd party IT management/service desk software.

Visit http://api.opmanager.com to know more on the API.

Installing SNMP Agent on Windows System

(Adapted from Windows help)

- Installing SNMP Agent on Windows XP/2000/2003
- Installing SNMP Agent on Windows NT
- Installing SNMP Agent on Windows 98

You need to know the following information before you install the Simple Network Management Protocol (SNMP) service on your computer:

- Community names in your network.
- Trap destinations for each community.
- IP addresses and computer names for SNMP management hosts.

To install SNMP on Windows XP, 2000, and 2003, follow the steps given below:

You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

- Click **Start**, point to **Settings**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
- In Components, click **Management and Monitoring Tools** (but do not select or clear its check box), and then click **Details**.
- Select the **Simple Network Management Protocol** check box, and click **OK**.
- Click **Next**.
- Insert the respective CD or specify the complete path of the location at which the files stored.

1. SNMP starts automatically after installation.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

To install SNMP in Windows NT, follow the steps given below:

- Right-click the **Network Neighborhood** icon on the Desktop.
- Click **Properties**.
- Click **Services**.
- Click **Add**. The Select Network Service dialog box appears.
- In the Network Service list, click **SNMP Service**, and then click **OK**.
- Insert the respective CD or specify the complete path of the location at which the files stored and click **Continue**.
- After the necessary files are copied to your computer, the Microsoft SNMP Properties dialog box appears.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

To install SNMP in Windows 98

Make sure your Windows 98 CD is in the drive. Then follow the steps given below:

- On the **Network** control panel, click **Add**.
- Double-click **Service** in the Select Network Component Type dialog box.
- Click **Have Disk** in the Select Network Service dialog box.
- Type the path to the "TOOLSRESKITNETADMINSNMP" directory on your computer's CD drive in the Install From Disk dialog box and then click **OK**.
- Select **Microsoft SNMP agent** from the **Models** list in the Select Network Service dialog box and then click **OK**.

This completes the installation process. This also implements the Host Resources MIB automatically. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP on Linux Systems

The installation of new version of SNMP is required only for versions prior to 8.

Download the latest rpm version of SNMP using the following URL:

http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.1.1-1.rh9.i686.rpm?download

Download the zip version of SNMP using the following URL:

http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz

To **install using the rpm**, follow the steps given below:

1. Login as "root" user.
2. Before installing the new version of net-snmp, you need to remove the earlier versions of net-snmp in your machine. To list the versions of net-snmp installed in your machine, execute the following command:

   ```
   rpm -qa | grep "net-snmp"
   ```
3. If there are already installed version in your machine, remove them using the command:

   ```
   rpm -e <version of net-snmp listed as the output for previous command> --nodeps
   ```
4. If there are no previously installed versions in your machine, then execute the following command to install the new version:

   ```
   rpm -i <new downloaded version of SNMP agent> --nodeps
   ```

To **install using the zip**, follow the steps given below:

Extract the file using following command:

tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
   - *./configure --prefix=<**directory_name**> --with-mib-modules="host"*

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

This completes the installation process. For configuring SNMP agents to respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP Agent on Solaris Systems

Download the latest version of SNMP using the following URL:

http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz

Extract the file using following command:

tar -zxvf ucd-snmp-4.2.6.tar.gz

To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:
   export PATH=<gcc path>:$PATH
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
   - *./configure --prefix=<****directory_name****> --with-mib-modules="host"*

     directory_name is the directory to install SNMP agent. Preferably choose a directory under /root. The directories /usr and /local might contain the files of an older version of SNMP and so do not choose these directories to ensure proper installation.
   - make
   - umask 022
   - make install

This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Configuring SNMP Agents

- Configuring SNMP agent in Windows XP/2000,2003
- Configuring SNMP agent in Windows NT
- Configuring SNMP agent in Linux versions prior to 8
- Configuring the Agent in Linux versions 8 and above
- Configuring SNMP agent in Solaris

Configuring SNMP Agent in Windows XP, 2000, and 2003 Systems

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

To configure SNMP agent in Windows XP and 2000 systems, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
5. Under Accepted community names, click **Add**.
6. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
7. In **Community Name**, type a case-sensitive community name, and then click **Add**.
8. Specify whether or not to accept SNMP packets from a host:
   - To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
   - To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name, IP or IPX address, and then click **Add** again.
9. Click **Apply** to apply the changes.

To configure SNMP traps, follow the steps given below:

1. Click **Start**, point to **Settings**, click **Control Panel**.
2. Under Administrative Tools, click **Services**.
3. In the details pane, right-click **SNMP Service** and select **Properties**.
4. In the **Traps** tab, under **Community name**, type the case-sensitive community name to which this computer will send trap messages, and then click **Add** to list.
5. Under **Trap destinations**, click Add.
6. In the **Host name, IP or IPX address** field, type host name or its IP address of the server (OpManager server) to send the trap, and click **Add**.
7. Repeat steps 5 through 7 until you have added all the communities and trap destinations you want.
8. Click **OK** to apply the changes.

Configuring SNMP Agent in Windows NT Systems

For details about installing SNMP agents in Windows systems, refer to Installing SNMP Agent on Windows Systems.

To configure SNMP agent in Windows NT systems, follow the steps given below:

- Click **Start**, point to **Settings**, click **Control Panel**.
- Under Administrative Tools, click **Services**.
- In the details pane, right-click **SNMP Service** and select **Properties**.
- In the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
- Under **Accepted Community Names**, click **Add**.
- In the **Community Names** box, type the community name to authenticate the SNMP requests.
- To move the name to the **Accepted Community Names** list, click **Add**.
- Repeat steps 6 and 7 for any additional community name.
- To specify whether to accept SNMP packets from any host or from only specified hosts, click one of two options:

- **Accept SNMP Packets From Any Host**, if no SNMP packets are to be rejected on the basis of source computer ID.
- **Only Accept SNMP Packets From These Hosts**, if SNMP packets are to be accepted only from the computers listed. To designate specific hosts, click Add, type the names or addresses of the hosts from which you will accept requests in the IP Host or IPX Address box, and then click Add.

- Repeat step 11 for any additional hosts.
- In the **Agent** tab, specify the appropriate information (such as comments about the user, location, and services).
- Click **OK** to apply the changes.

Further, the SNMP Agent running Windows NT does not respond to Host Resource Data, by default. To include this support, you should have Windows NT Service Pack 6 & above. Verify this and then follow the steps given below:

- Extract the NTHR-MIB.zip available at http://bonitas.zohocorp.com/opmanager/07Jul2010/NTHR-MIB.zip into C:WinNTsystem32 folder.
- Double click on the registry files to import the mibs into Windows registry.
- Restart your Windows NT box.

To Configure SNMP Traps, follow the steps given below:

- Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
- In the details pane, click **SNMP Service**, and then click **Properties**.
- Click the **Traps** tab.
- To identify each community to which you want this computer to send traps, type the name in the **Community Name** box. Community names are case sensitive.
- After typing each name, click **Add** to add the name to the list.
- To specify hosts for each community you send traps to, after you have added the community and while it is still highlighted, click **Add** under Trap Destination.
- To move the name or address to the Trap Destination list for the selected community, type the host name in the **IP Host/Address or IPX Address** box, and then click **Add**.
- Repeat step 10 for any additional hosts.
- Click **OK** to apply the changes.

Configuring the Agent in Linux versions prior to 8

For details about installing SNMP agents in Linux systems, refer to Installing SNMP Agent on Linux Systems.

- Stop the agent if it is running already using the command:
  `/etc/rc.d/init.d/snmpd stop`
- Make the following changes in **/etc/rc.d/init.d/snmpd** file
  - Replace the line
    daemon /usr/sbin/snmpd $OPTIONS
    with
    daemon /root/ucd_agent/sbin/snmpd $OPTIONS
  - Replace the line
    killproc /usr/sbin/snmpd
    with
    killproc /root/ucd_agent/sbin/snmpd

    This is to choose the current installed version while starting and stopping the SNMP agent.
- Start the agent using the command */etc/rc.d/init.d/snmpd start*.

Configuring the Agent in Linux versions 8 and above

On Linux versions 8 and above, the latest version of SNMP will already be available. You need to just make the following changes in **snmpd.conf** file:

- Insert the line
  ```
  view    allview       included   .1.3.6
  ```
  next to the line
  ```
  #       name          incl/excl     subtree         mask(optional)
  ```
- Change the line
  ```
  access  notConfigGroup ""      any       noauth    exact  systemview none none
  ```
  next to the line
  ```
  #       group         context sec.model sec.level prefix read   write  notif
  ```
  as

```
access  notConfigGroup ""      any       noauth    exact  allview none none
```

- Then restart the snmp agent using the following command:

  ```
  /etc/rc.d/init.d/snmpd restart
  ```

Configuring the Agent in Solaris Systems

For details about installing SNMP agents in Solaris systems, refer to Installing SNMP Agent on Solaris Systems.

- Stop the agent if it is running already using the following command:

  ```
  /etc/init.d/init.snmpdx stop
  ```

- Make the following changes in **/etc/init.d/init.snmpdx** file
  - Replace the lines

    ```
    if [ -f /etc/snmp/conf/snmpdx.rsrc -a -x /usr/lib/snmp/snmpdx ]; then
    /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -d 3 -f 0
    fi
    ```

    with

    ```
    <Installation Directory>/sbin/snmpd
    ```

  - Replace the line

    ```
    /usr/bin/pkill -9 -x -u 0 '(snmpdx|snmpv2d|mibiisa)'
    ```

    with

    ```
    /usr/bin/pkill -9 -x -u 0 '(snmpd)'
    ```

- Restart the agent using the following command:

  ```
  /etc/init.d/init.snmpdx start.
  ```

Configuring SNMP Agent in Cisco Devices

For configuring SNMP agents in Cisco devices, you need to log into the device and switch to privileged mode.

Use the following set of commands listed below to enable SNMP:

To enable SNMP:

From the command prompt, run the following commands:

```
#configure terminal
#snmp-server community <community_string> rw/ro (example: snmp-server community public ro)
#end
#copy running-config startup-config
```

To enable trap:

Again, from the command prompt, run the following commands:

```
#configure terminal
#snmp-server enable traps snmp authentication
#end
#copy running-config startup-config
```

To set OpManager as host:

Run the following commands from the command prompt:

```
#configure terminal
#snmp-server host <OpManager server running system's IP> <Trap community string> snmp (example: snmp-server host 192.168.9.58 public snmp)
#end
#copy running-config startup-config
```

Configuring SNMP Agent in Lotus Domino Server

The Domino SNMP Agent is configured as a Windows Service and is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP and Windows SNMP Services before beginning the upgrade process.

- Stop the LNSNMP and SNMP services. Enter these commands:

  ```
  net stop lnsnmp
  net stop snmp
  ```

- Configure the Lotus Domino SNMP Agent as a service. Enter this command:

  ```
  lnsnmp -Sc
  ```

- Start the SNMP and LNSNMP services. Enter these commands:

  ```
  net start snmp
  net start lnsnmp
  ```

Configuring SNMP Agent in MSSQL Server

Verify whether SNMP agent is running in the server. If the agent is not installed in the server, refer to Installing SNMP Agent on Windows System and Configuring SNMP agents for installing and configuring SNMP agent.

Then, start the SQLSERVERAGENT service following the steps given below:

In **Windows 2000/XP**:

- Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Computer Management**.
- In the console tree, click **Services and Applications** and then click **Services**.
- Right-click **SQLSERVERAGENT** and click **Start**.

In **Windows NT**:

- Right-click on the **Network Neighborhood** icon on the Desktop.
- Click **Properties**.
- Click **Services**.
- Right-click **SQLSERVERAGENT** and click **Start**.

Configuring SNMP Agent in Oracle Server

To collect data from the Oracle servers and to receive traps from them using OpManager, you need to install and configure Oracle Intelligent Agent. The Oracle Intelligent Agent supports SNMP, allowing third-party systems management frameworks to use SNMP to receive SNMP traps directly from the Agent. By configuring the Agent to recognize SNMP requests from the master agent, third-party systems can gather relevant data.

In Windows machines

1. Once you have installed and configured the SNMP agents in your Windows machines, you have to integrate SNMP with Intelligent agent. This requires Oracle Peer SNMP Master Agent and SNMP Encapsulator Agent to be installed in the Oracle server. Note that these agents must be the same version as the Intelligent Agent and installed in the same ORACLE_HOME.

After the installation completes, the following new NT services will be created: Oracle SNMP Peer Encapsulator Oracle Peer SNMP Master Agent.

If you do not install the Intelligent Agent software in the default $ORACLE_HOME, the names of all the services will begin with the following: Oracle<home name>

For SNMP master agent to communicate with both the standard SNMP service and the Intelligent Agent, the SNMP services file must be configured properly.

Specify an unused port where the encapsulated agent, Microsoft SNMP Service, should be listening. Microsoft SNMP Service typically uses port 1161. The port is specified in the SERVICES file located in the NT_HOMESYSTEM32DRIVERSETC directory.

Make sure that you have the following lines in the file:

```
snmp 1161/udp snmp
snmp-trap 1162/udp snmp
```

Note: If an entry for SNMP already exists in the file, change the port from 161 (default number) to another available port (1161 in this example).

2. In the same location, check that the HOSTS and LMHOSTS.SAM files contain the mappings of IP addresses to host names for all computers in the SNMP setup. System performance will improve if more computer addresses can be resolved locally. Even if you use DHCP and WINS, adding the IP addresses will speed up the SNMP integration.