# Table of contents

## INTRODUCTION
- Key Features ......................................................... 5
- Monitoring Capabilities .................................................. 7
- What's New in Release 6.6 .................................................. 9

## INSTALLATION AND SETUP
- System Requirements .................................................. 13
- Installing and Uninstalling ........................................... 14
- Licensing Applications Manager .................................. 18
- Using Update Manager ................................................ 19
- Starting and Shutting Down Applications Manager .......... 20

## GETTING STARTED
- Understanding Applications Manager ......................... 23
- Prerequisites for Applications Manager ....................... 24
- Working with Applications Manager ............................... 29

## WORKING WITH MONITOR GROUPS
- Using Monitor Group Wizard ..................................... 31
- Creating New Monitor Group .................................... 32
- Associating Monitor with Monitor Groups .................... 33
- Deleting Monitor from Monitor Groups ....................... 34
- Deleting a Monitor Group .......................................... 35

## CREATING NEW MONITOR
- Application Servers .................................................. 37
- Database Servers ...................................................... 45
- Services ...................................................................... 48
- Mail Servers .............................................................. 50
- Web Services .............................................................. 52
- Servers ...................................................................... 54
- HTTP URL Monitors .................................................. 56
- Custom Monitors ....................................................... 60
- Script Monitors ........................................................ 62
QEngine Script Monitors........................................................................................................... 63
Web Transaction Monitor........................................................................................................... 64

MONITOR INFORMATION ..................................................................................................... 65
Application Servers.................................................................................................................. 67
Microsoft .NET.......................................................................................................................... 68
JBoss Servers............................................................................................................................ 70
Oracle Application Servers....................................................................................................... 72
Tomcat Servers.......................................................................................................................... 74
WebLogic Servers..................................................................................................................... 76
WebSphere Servers................................................................................................................... 78
Database Servers....................................................................................................................... 80
MySQL DB Servers.................................................................................................................... 81
Oracle DB Servers..................................................................................................................... 83
MS SQL DB Servers.................................................................................................................. 87
IBM DB2 DB Servers................................................................................................................ 90
Services.................................................................................................................................... 93
Mail Servers............................................................................................................................. 94
Web Services........................................................................................................................... 96
Servers..................................................................................................................................... 98
HTTP URL Monitors.............................................................................................................. 101
Custom Monitors..................................................................................................................... 102
Adding Attributes ................................................................................................................... 102
Adding JMX MBeans Attributes......................................................................................... 103
Adding SNMP OID Attributes............................................................................................. 105
Script Monitors....................................................................................................................... 107
QEngine Script Monitors........................................................................................................ 109
Web Transaction Monitors...................................................................................................... 111
Web Transaction Agent.......................................................................................................... 112
Web Transaction Metrics........................................................................................................ 113

CONFIGURING ALERTS ........................................................................................................ 115
Viewing and Configuring Alerts Globally............................................................................. 116
Creating Threshold Profile..................................................................................................... 117
Creating Actions...................................................................................................................... 118
Sending E-mail....................................................................................................................... 119
Sending SMS........................................................................................................................ 120
Executing Program................................................................................................................. 121
## Sending Trap ............................................................................................................................... 122
## Execute MBean Operation........................................................................................................... 123
## Log a Ticket ................................................................................................................................. 125
## Replaceable Tags........................................................................................................................126
## Associating Threshold and Action with Attributes............................................................ 127
## Bulk Alerts Configuration ................................................................................................. 128
## Configuring Dependencies .............................................................................................. 129
## Configuring Retry Polls .................................................................................................... 130

### VIEWING REPORTS ............................................................................................. 131

- Grouping of Reports ........................................................................................................ 132

### PERFORMING ADMIN ACTIVITIES...................................................................... 136

- Action / Alert Settings ...................................................................................................... 137
- Availability Settings .......................................................................................................... 138
- Network Discovery ........................................................................................................... 139
- Bulk Configuration of Monitors ......................................................................................... 140
- Performance Polling ........................................................................................................ 141
- Windows Event Log Rules .................................................................................................. 142
- Global Settings ................................................................................................................ 143
- Configure Mail Server ...................................................................................................... 145
- Configure Proxy ................................................................................................................ 146
- Upload Files/Binaries ........................................................................................................ 147
- User Administration ........................................................................................................ 148
- Personalize Web Client ................................................................................................... 149
- Add On - Products Settings ............................................................................................. 150
- Database Retention ......................................................................................................... 151
- Google Map Business View ............................................................................................. 152
- Downtime Scheduler ........................................................................................................ 153
- SNMP Trap Listener ........................................................................................................ 154
- Schedule Reports ............................................................................................................ 155

### MANAGER CONSOLE .......................................................................................... 156

#### INTEGRATING WITH SERVICEDESK PLUS ....................................................... 158

#### TECHNICAL SUPPORT AND PRODUCT INFORMATION................................. 159

#### GLOSSARY ........................................................................................................... 162

#### FAQ........................................................................................................................ 165
APPENDIX.................................................................................................................. 174

Applications Manager Home....................................................................................... 175
Icon Representation..................................................................................................... 176
Alert Details ................................................................................................................ 178
Reconfiguration Details.............................................................................................. 179
Network View ............................................................................................................. 180
Miscellaneous Links Details....................................................................................... 181
Data Collection - Host Resource ................................................................................ 182
SNMP Agent Installation............................................................................................. 183
SNMP Agent Configuration........................................................................................ 186
Security/Firewall Requirements ................................................................................ 189
Introduction

AdventNet ManageEngine™ Applications Manager is a comprehensive application used to monitor heterogeneous business applications such as Web applications, application servers, Web servers, databases, network services, systems, etc. It provides remote business management to the applications or resources in the network. It is a powerful tool for the system and network administrators, helping them monitor any number of applications or services running in the network without much of manual efforts.

Applications Manager offers out-of-the-box discovery, availability, health, performance and fault management, and reporting of multi-vendor applications.

Alerts are generated to notify the faults in the application and are configured to trigger actions, such as notifying the user through e-mail, SMS, trap, executing a command and invoking a MBean operation. Through alerts, you can identify the root cause of any problem in the network with just a few clicks. Additionally, the flexible architecture of the Applications Manager allows you to manage any application (J2EE or J2SE) that exposes management information via JMX or SNMP through custom applications.
Key Features

The following are some of the key features of this release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Server Monitoring</strong></td>
<td>Monitors Microsoft .NET, WebLogic, WebSphere, Tomcat, Oracle Application server, JBoss application servers and also Web-based applications such as Servlets, JSP, and EJB of the application servers.</td>
</tr>
<tr>
<td><strong>Web Transactions Monitoring</strong></td>
<td>Monitor Web Transactions end to end, with performance metrics of all components starting from URLs to SQLs.</td>
</tr>
<tr>
<td><strong>Database Monitoring</strong></td>
<td>Supports monitoring of MySQL, Oracle, IBM DB2 and MS SQL.</td>
</tr>
<tr>
<td><strong>Host Resource Monitoring</strong></td>
<td>Monitors the performance of Windows, Linux, Solaris, HP Unix, Tru64, Unix IBM AIX and FreeBSD servers. Also monitors Event Logs for Windows.</td>
</tr>
<tr>
<td><strong>Script Monitoring</strong></td>
<td>Ad-hoc Windows/Linux custom scripts, used in-house can be managed from the same web console. Additionally, AdventNet QEngine, a test automation suite has been integrated in Applications Manager.</td>
</tr>
<tr>
<td><strong>Services Monitoring</strong></td>
<td>Monitors Services such as FTP, Telnet, RMI adaptor, TCP port, etc.</td>
</tr>
<tr>
<td><strong>Mail Servers Monitoring</strong></td>
<td>Monitors Mail servers (including SMTP servers and POP servers) and Microsoft Exchange Server.</td>
</tr>
<tr>
<td><strong>WebServices Monitoring</strong></td>
<td>Monitors Apache, IIS, PHP and other webservers.</td>
</tr>
<tr>
<td><strong>HTTP URL Monitoring</strong></td>
<td>Monitors any HTTP or HTTPS -based URL of web pages.</td>
</tr>
<tr>
<td><strong>Custom Application Management</strong></td>
<td>Groups data sources from multiple resources and displays them in a common place. The data sources can be JMX MBeans and SNMP agents.</td>
</tr>
<tr>
<td><strong>Fault Management</strong></td>
<td>Sends ‘Alerts’ based on the monitored attributes. These can be escalated through e-mail / SMS / trap/ MBean Operation/ execute a program.</td>
</tr>
<tr>
<td><strong>Performance Reports</strong></td>
<td>The performance of the monitored application is depicted in the form of graphs and charts for easy analysis. Its powerful reporting mechanism enables you to analyze the trends over a period. Scheduling of reports is also possible.</td>
</tr>
<tr>
<td><strong>Intuitive Web Client</strong></td>
<td>Allows you to perform admin activities through Web browser interface. You can also monitor and view attributes such as the health and availability of the monitors.</td>
</tr>
<tr>
<td><strong>Holistic view to Monitor Group</strong></td>
<td>Manages a wide range of business applications and network services. It provides you the flexibility to group the application and its related services to be monitored as a single unit.</td>
</tr>
<tr>
<td><strong>Graphical Representation of Attribute Statistics</strong></td>
<td>The attribute details are represented through graphs that provides an easy approach to understand the &quot;attribute vs time&quot; statistics for one hour. Also the icons and provided in the graphs represent details about the statistics for 7 days and 30 days respectively.</td>
</tr>
<tr>
<td><strong>Scalable Architecture</strong></td>
<td>It's scalable architecture provides you the ability to monitor a variety of Monitors. It uses a blend of both agent-based monitoring and agent-less monitoring depending on the need.</td>
</tr>
<tr>
<td><strong>Root Cause Analysis</strong></td>
<td>Provides details on the different severity levels by identifying its reason/cause.</td>
</tr>
<tr>
<td><strong>Business Service Management</strong></td>
<td>Manager Console helps the Manager to have an integrated high-level view of the Business Infrastructure. Location intelligence is added via Google Map Business View.</td>
</tr>
</tbody>
</table>
Monitoring Capabilities

This section lists the different types that Applications Manager can monitor. The types are divided into categories based on the type of system or component.

1. Application Servers
   - Microsoft .NET
   - JBoss Servers
   - Oracle Application Servers
   - Tomcat Servers
   - WebLogic Servers
   - WebSphere Servers

2. Database Servers
   - MySQL Database Servers
   - Oracle Database Servers
   - MS SQL Database Servers
   - IBM DB2 Database Servers

3. Services
   - JMX [MX4J / JDK 1.5]
   - Service Monitoring
   - AdventNet JMX Agent - RMI Adapter
   - SNMP
   - Telnet

4. Mail Servers
   - Microsoft Exchange Server
   - Mail Server

5. Web Services
   - Apache Server
   - IIS Server
   - PHP
   1. HTTP URL Monitors and HTTP URL Sequence
      - Web Server

6. Servers
   - Linux
   - Windows
   - Solaris
   - IBM AIX
   - HP Unix / Tru64 Unix
   - Free BSD
7. Custom Monitors
   - JMX / SNMP Dashboard
   - Script Monitor
   - QEngine Script Monitor

8. Transaction Monitors
   - Web Transactions Monitor
What's New in Release 6.6

- Support for Oracle Application Server Monitoring
- Support for Tru64 Unix Monitoring
- Support for Windows Event Log monitoring
- Support for LAMP Edition and Database Edition of ManageEngine Applications Manager
- Option to schedule daily, weekly, monthly performance and availability reports
- Option to copy and paste the configuration of one monitor to create new monitors
- Bulk update of usernames and passwords of monitors
- Ability to Manage / Unmanage a monitor
- Option to configure the number of polls for performance data collection
- Bulk alert configuration for attributes
- More configuration support for Google Maps Business Views

What's New in Release 6.0.5

- Integration of Google Maps Business View
- Support for Weblogic 9.1
- Support for JBoss 4.0.3
- Multilingual support for Simplified Chinese and Japanese languages
- PDF report generation for attributes is provided
- Enhanced Web Client

What's New in Release 6.0.4

- Support for monitoring Microsoft .NET
- Support for monitoring WebLogic 9.
- Support for monitoring Web Transactions.
- Support for monitoring Oracle RAC.
- Integration of ManageEngine ServiceDesk Plus to track the alerts generated as trouble tickets.
- NTLM support is provided in URL monitoring.
- Reporting enhancements like Downtime History report of individual monitors and Summary Report are provided.
- Various usability enhancements like configuring prerequisites for monitoring are provided at the initial stage itself.
- Option to configure database retention parameters.

What's New in Release 6.0.3

- Support for Monitoring Microsoft Exchange Server.
- Support for Monitoring of FreeBSD Operating Systems.
- Support for Monitoring JBoss 4.0.2.
- Support for Telnet Monitoring is provided.
Integration of AdventNet's QEngine - a platform independent Test Automation tool used for Web Functionality, Web Performance, Java Application Functionality, Java API, SOAP, Regression, and Java Application Performance testing.

- Standalone Enhanced URL Recorder is provided.
- SSL support for Apache, IIS and PHP.
- Consoles for Manager provided to maintain SLAs.
- Option to associate multiple users to single Monitor Group is provided.
- Alert Enhancements like Pick/Unpick alerts, Annotation of alerts have been provided.
- Polls to retry can be configured individually for any attribute of a Monitor.
- Multiple varbind support in alert messages is provided.
- Option to export reports to CSV and PDF formats.

### What's New in Release 6.0.2

- Support for Monitoring IBM AIX servers.
- Support for Monitoring HP Unix Servers.
- Support for Script Monitoring is provided.
- Support for PHP Monitoring is provided.
- WebSphere 6.0 Monitoring support is provided.
- WebSphere Monitoring in Network Deployment mode is supported.
- Maintenance Task Scheduler Provided.
- SNMP Trap Listener provided.
- JMX Notification Listener Provided.
- Introduction of new role - "User", in addition to the existing Operator & Administrator roles.
- Replaceable Tags enhancement provided in actions.
- Support for String data type for defining threshold values.
- Option to be execute an action (like email) repeatedly, till a monitor returns to normalcy.
- Alert Template feature for bulk alert configuration.
- Support for JBoss SSL.
- Custom Time Period reports provided.
- Option to delete known downtime reports provided.

### What's New in Release 6.0.1

- Support for Monitoring Apache WebServers.
- Support for Monitoring IIS WebServers.
- Support for IBM DB2 Database Server Monitoring.
- JMX MBean Operation Support.
- Support for Monitoring JBoss 4.x.
- Support for Tomcat SSL.
What's New in Release 6

- Support for Monitoring WebSphere Application Server 5.x
- Support for Monitoring JBoss Application Server 3.2.x
- Support for Monitoring Tomcat Application Server
- Support for Monitoring WebLogic 8.1 Application Server
- Support for Monitoring MS SQL Database
- Support for Monitoring Oracle 10g Database
- Support for Monitoring MySQL Database
- Support for Monitoring Mail servers (SMTP, POP)
- Support for Monitoring Web servers
- Support for Monitoring Network Services like ftp, telnet, tcp port, etc
- Support for Monitoring Websites (URL, URL sequence, URL content monitors)
- SNMP based custom application monitoring
- JMX based custom application monitoring for MX4J / JDK 1.5, WebLogic JMX, JBossMX, WebSphere JMX
- Intuitive Web client support
- Unified view of monitors using Monitor Group
Installation and Setup

You can install Applications Manager with ease, by going through the following sections:

- System Requirements
- Installing and Uninstalling
- Licensing
- Using Update Manager
- Starting and Shutting Down
System Requirements

This section lists the minimum requirements for installing and working with Applications Manager.

Hardware Requirements

Performance of Applications Manager depends considerably on the CPU and memory of the system. The following table describes the minimum configuration of the system running the product.

<table>
<thead>
<tr>
<th>Operating Platform</th>
<th>Processor Type</th>
<th>Processor Speed</th>
<th>Memory</th>
<th>Hard Disk Space Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Pentium IV</td>
<td>1.4 GHz</td>
<td>512 MB RAM</td>
<td>250 MB*</td>
</tr>
<tr>
<td>Linux</td>
<td>Pentium IV</td>
<td>1.4 GHz</td>
<td>512 MB RAM</td>
<td>250 MB*</td>
</tr>
</tbody>
</table>

- Higher configuration of hardware would enable you to manage more monitors.
* While going into production 1GB is recommended.

Software Requirements

Applications Manager is optimized for 1024 x 768 resolution and above.

Supported Operating Systems

Applications Manager is tested to support the following operating systems and versions:

- Windows 2000 Server / Professional / XP / 2003
- RedHat Linux 8.0 / 9.0
- Enterprise Linux 2.1 or Debian

Supported Browsers

The supported browsers are

- Mozilla 1.6 and above
- Internet Explorer 5.5 and above
- FireFox 1.x
Installing and Uninstalling

The following are the Applications Manager product versions.

- Professional Edition (Trial)
- Free Edition
- Professional Edition (Registered)

**Note:** Click the list to know the supported monitors in the different versions - LAMP Edition, Database Edition in comparison with Professional Edition.

**Free Edition:** This allows you to monitor Five monitors (This excludes the Monitors discovered by default). The Free Edition never expires and you get the functionalities of Professional Edition except for network discovery and creation of users.

**Professional Edition (Trial):** You can avail 30 days of free evaluation with no restrictions on number of monitors.

**Professional Edition (Registered):** This is the registered version of the product. AdventNet provides the Registered user file after you purchase the product. To get the registered user file, e-mail to sales@adventnet.com.

**Note:** You can upgrade the Professional Edition Trial and Free Edition to Professional Registered Edition. This is applicable, if you have purchased AdventNet's Applications Manager and hold the registered license key. To upgrade your license, refer Licensing Applications Manager.

To Install Applications Manager in Windows (.exe)

1. Execute the downloaded file. The Installation Wizard is displayed. Click **Next** to continue.
2. Read the license agreement and click **Yes**.
3. Select the **language** in which you wish to install Applications Manager. The options are English, Simplified Chinese, Traditional Chinese, and Japanese.
4. Provide the location where the Applications Manager should be installed in your machine. Click **Browse** to provide a different location of installation. Click **Next**.
5. Specify the name of the Folder to be placed in Program Folder. The default is **ManageEngine Applications Manager 6**. Click **Next**.
6. Specify the port at which web server has to be started. By default, it is **9090**. This is the port at which you will connect the web client.
7. If you want to install Applications Manager as a service, select the 'Install Applications Manager as Service' option and click **Next**.

**Note:** For installing as service, you need to have administrative privileges in that system. [More Information on 'Manually Installing Applications Manager as Service']. Incase, you did not select this option while installing the Applications Manager, you can then install Applications Manager as service by invoking the **installService.bat** found under <home>/bin. For invoking installService.bat, you must have started Applications Manager atleast once.

With this service, the Apache server bundled with Applications Manager product is also installed as a service - **ApacheApplications Manager**. The startup type is set as 'Manual', by default, and you are not required to handle this service. Applications Manager will handle it.

8. You have an option to fill up a **registration form** for Technical Support.
9. Current Settings is displayed in the next screen. If you need to make changes, click **Back**, else click **Next**. The installation begins.
10. The next screen prompts for the product edition (Professional - Trial, Professional - Registered User and Free Edition). Select the preferred edition to install. If Professional - Registered User is selected, you will be prompted to specify the license file that you have obtained.

11. Finally, you would be given two options - 1. To view the ReadMe file 2. To launch Applications Manager immediately.

12. Click Finish to complete the installation process.

To Install Applications Manager in Linux (.bin)

1. Download the product for Linux.
2. Execute the downloaded file. The Installation Wizard is displayed. Click Next to continue.
3. The next screen prompts for the product edition (Professional - Trial, Professional - Registered User, and Free Edition). Select the preferred edition to install. If Professional - Registered User is selected, you will be prompted to specify the license file that you have obtained. Read the license agreement and click Next.
4. Select the language in which you wish to install Applications Manager. The options are English, Simplified Chinese, Traditional Chinese, and Japanese.
5. Provide the location where the Applications Manager should be installed in your machine. Click Next.
6. Specify the port at which web server has to be started. By default, it is 9090. This is the port at which you will connect the we client.
7. Specify a password for the user 'admin'. By default, it is 'admin'. This is the password using which you will login to the web client.
8. Current Settings is displayed in the next screen. If you need to make changes, click Back, else click Next. The installation begins.
9. Click Finish to complete the installation process.

Note: You can install Applications Manager via Command Line also. If the file name is ManageEngine_ApplicationsManager_6_linux.bin, then type the following command in the command prompt

/ManageEngine_ApplicationsManager_6_linux.bin -console

Execution of this command would take you through the installation process.

Trouble Shooting Installation

In case of any errors during installation, follow the steps given below to produce the logs files (applicable only for Linux).

1. Create a text with the same name as that of the installer and with extension as ".sp". i.e, For <File Name>.bin, create a text file named <File Name>.sp
   Example: If the file name is ManageEngine_ApplicationsManager_6_linux.bin, create a text file named ManageEngine_ApplicationsManager_6_linux.sp
2. Open the ".sp" text file in an editor, add is.debug=1 as the content.
3. Save the ".sp" text file in the same directory where the binary file resides.
4. Change to the directory where the binary file is present by executing cd command
5. Invoke the installer as
   ./<File Name>.bin -is:javaconsole -is:log log.txt
6. The above command will create the log file named log.txt. Mail the log file to support@appmanager.com.

Note: If the execution of the installation command throws an error such as "there may not be enough temporary space available in the temp folder", then execute the file with the argument as
Uninstalling Applications Manager

Windows

Click Start > Programs > ManageEngine Applications Manager 6 > Uninstall Applications Manager

Linux

Execute the command ./uninstaller.bin from the <Applications Manager Home>_/uninst directory.

List of supported monitors in the different versions - LAMP Edition and Database Edition in comparison with Professional Edition. (* denotes supported monitors)

<table>
<thead>
<tr>
<th>Monitors</th>
<th>LAMP</th>
<th>Database</th>
<th>Professional Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft .NET</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>JBoss</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Oracle Application Server</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Tomcat</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>WebLogic</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>WebSphere</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Java Web Transactions Monitor</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Mail Server</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>MySQL</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Oracle</td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Apache</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>IIS</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>PHP</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>URL Monitor</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>URL Sequence</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Web Server</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>JMX [MX4J / JDK1.5]</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Service Monitoring</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>RMI Adaptor</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>SNMP</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Telnet</td>
<td>*</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>JMX/SNMP Dashboard</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>QEngine Script Monitor</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Feature</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Script Monitor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM AIX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FreeBSD</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>HP-UX / Tru64 Unix</td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Linux</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Sun Solaris</td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Windows</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Manager Console (BSM)</td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Network Discovery</td>
<td></td>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>
Licensing Applications Manager

When you have purchased the registered license file from us, you need to apply the license file over the existing version. This section explains the procedure to apply the new license file.

To apply the new license file from the web client

A quick way to apply the new license file is from the web client.

1. In the web client, click **Register** link provided on top.
2. A **Register Applications Manager** pop-up is displayed.
3. Click **Browse** button and locate the file (License.xml) in your local machine.
4. Click **Register**.

Your existing version is now changed to Professional Edition - Registered.

**Note:** The **Register** link on top would disappear for the users who have applied the registered license. If the registered customers, want to upgrade their license further, they can use the **Product License** link under Applications Manager Server Settings in Admin tab.

To apply the new license file using License Manager

The license manager comes handy when your license has already expired and you are not able to access the web client.

1. Invoke the **updateLicense.bat/.sh** file located in the `<Applications Manager Home>/bin` directory. The License Manager UI is displayed.
2. Click **Browse** button and locate the file (License.xml) in your local machine.
3. Click **Next**.
4. Click **Finish**.
5. Re-start the Applications Manager server.

**Note:** To invoke License Manager via **Command Line**, use the following command `<updateLicense.bat/.sh -c>`

Please contact us at support@appmanager.com for any technical query.
Using Update Manager

The Update Manager is a tool which is used for installing the service packs (.ppm file) over Applications Manager. The service pack may contain certain bug fixes and new feature additions. This document explains about how to use the Update manager to install service packs over Applications Manager.

**Note:** The Update Manager also has some useful validation incorporated. This validation includes compatibility checks. You cannot use update manager to install an incompatible service pack. For example, you cannot install a service pack of another product in Applications Manager or a service pack of one version of Applications Manager in another version.

**Installing Service Pack using Update Manager**

1. Run `updateManager.bat/sh` file located in the `<Applications Manager Home>/bin` directory or invoke `Start > Programs> ManageEngine Applications Manager 6 > Update Manager` in Windows. The Update Manager tool is displayed. Click `Update`.

2. Provide the service pack (.ppm file) by clicking the `Browse` button. Only compatible service pack file will be opened. Once the file is specified, other buttons such as Readme and Install are enabled.

3. Click the `Readme` button and the Readme file related to the service pack is displayed in a separate window.

4. Click `Install`. This opens a new panel where the installation process is displayed. On completion, a message “Service Pack installed successfully” is displayed and the service pack is listed in the **Installed Patches** section.

To uninstall the service pack, click the **Uninstall** button and to know the service pack details, click the **Details** button in Update Manager.

**Installing Service Pack using Update Manager (Command Line Option)**

1. Under `<Applications Manager Home>/bin`, execute the following command.

   ```
   updateManager.bat -c in Windows  
   sh updateManager.sh -c in Linux
   ```

Using this command line option, you can install or uninstall a service pack or view its details. Press 'i' to install and specify the absolute path of the service pack file in your machine.
Starting and Shutting Down Applications Manager

Starting Applications Manager

Once installation is successful, you can start the Applications Manager by following the instructions provided for different operating systems.

To start Applications Manager

In Windows

- Click Start > Programs > ManageEngine Applications Manager 6 > Applications Manager Start (or)
- Invoke the batch file `startApplicationsManager.bat` file located in the `<Applications Manager Home>` directory.

Once the server is initialized, a tray icon is placed in the Windows system tray. After the server is started completely the icon changes to and a message "Server Ready for Monitoring!" is displayed over the icon. Right-click on the Applications Manager tray icon to connect to the web client or stop Applications Manager.

Starting Applications Manager as a Windows Service

In Windows, you can start Applications Manager as a service. With this feature you can start the Applications Manager server automatically when the Windows system starts.

By default, during product installation, you can choose to install it as a service (More on Installation). If you have not enabled it then, use the following option to setup Applications Manager as a service.

1. Go to `<Applications Manager Home>/bin` directory, execute the file `installasservice.bat`. On executing this file, 'ManageEngine Applications Manager' service is added in Windows Services and the startup type is set as 'Automatic', by default. (To ensure if it is installed as service, check for the 'Services' under 'Windows Administrative Tools'). **Note:** For installing Applications Manager as service, you need to have administrative privileges in that system.

2. Now, when you start Windows system, Applications Manager is automatically started. You can swap between Automatic and Manual modes.

To uninstall this service, go to `<Applications Manager Home>/bin` directory, execute the file `uninstallservice.bat`.

In Linux

Execute the `startApplicationsManager.sh` file in the `<Applications Manager Home>` directory.

💡 Troubleshoot: Having trouble starting Applications Manager? Refer to the online Troubleshooting section.

Shutting Down Applications Manager

To shutdown Applications Manager

In Windows

- Click Start > Programs > ManageEngine Applications Manager 6 > Applications Manager Shutdown (or)
o Invoke `shutdownApplicationsManager.bat` file located in the `<Applications Manager Home>` directory (or)

o Right-click on the Applications Manager tray icon and click Stop Applications Manager.

**In Linux**

Use `shutdownApplicationsManager.sh` script located in the `<Applications Manager Home>` directory to shutdown Applications Manager.
Getting Started

In Windows, by default, when Applications Manager is started, the default browser, as configured in your system, is invoked and the login screen is displayed. Login by specifying the authentication details. The default user name and password are "admin" and "admin" respectively. To know more about the different types of user access to the product, refer to the User Administration section of Performing Admin Activities.

In Windows, If you do not want the client to open by default, follow the steps given below to disable it.

1. Edit **AMServer.properties** file located in the `<Applications Manager Home>/conf` directory.
2. Set the value of **am.browser.startup** as **false** (by default, it is **true**).

After this configuration, when you restart the server the next time, the web client will not be invoked automatically. In Linux, by itself, the client will not open by default.

To login to Web Client when it is not opened by default

1. Connect to the Applications Manager through any browser with the host name and port number, say **http://localhost:9090**, where 9090 is the default port number.
   
   **In Windows,**
   a. Click **Program Files > ManageEngine Applications Manager > Applications Manager Web Console**.
   b. Right-click the Applications Manager tray icon and click **Start Web Client**.

1. Then log in to the Applications Manager by filling in the User Authentication details.

   **Note:** You can also use the **startWebConsole.bat or sh** file available at the `<Applications Manager Home>` directory that opens a default browser of the localhost and connect to the Applications Manager at **http://localhost:9090**. Ensure that the Applications Manager is started before executing this file.

Browse through the following topics which would help you understand Applications Manager better and work with it easily.

- Understanding Application Manager
- Working with Application Manager
Understanding Applications Manager

Applications Manager is a user-friendly intuitive tool enabling system and network administration. It is a single, powerful interface that enhances Monitor Group management by monitoring, alerting, and reporting on the availability, health, response time etc. of the Monitor running in a network. Now let us have an overview of Applications Manager.

Applications Manager is a comprehensive tool to view data monitored by the Monitor Groups. You can find seven module tabs at the top which are explained as follows:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intro</td>
<td>Introduction Page of Applications Manager. Any novice user can work with the product by going through the introduction part and understanding the terms used in Applications Manager.</td>
</tr>
<tr>
<td>Home</td>
<td>Lists all the Monitor Groups created using the Applications Manager and their details, a table representing the availability and health details for the different Monitor Type, and graphical representation of the Monitor Group with most critical alerts. You can have a detailed view by clicking on the respective parameters and icons.</td>
</tr>
<tr>
<td>Monitors</td>
<td>Lists all the Monitor Types supported and provides the number of Monitor being discovered in the network. You can also click on the Monitor Types to view information of their Monitor.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Lists the alerts generated by the Monitor and their attributes, based on predefined thresholds. The view is customizable such that you can view alerts for all or for particular application or Monitor Type, list 10/25/50/75/100/125 entries in a single view, etc.</td>
</tr>
<tr>
<td>Reports</td>
<td>Lists the Monitor Groups and the different Monitor Types for which the reports are generated. Reports can be viewed based on attributes listed for the corresponding Monitor Type.</td>
</tr>
<tr>
<td>Support</td>
<td>Provides information on getting assistance from the Applications Manager Technical center. It also provides monitoring information on Applications Manager which monitors itself.</td>
</tr>
<tr>
<td>Admin</td>
<td>Lists the admin operations such as creating new application, new Monitor, etc. to be performed for monitoring.</td>
</tr>
</tbody>
</table>

The left frame consists of links for easy navigation and the top frame consists of links such as Talk back, Help, Personalize etc. common in all the screens. To know more details on these links and icon representation, refer to the Appendix section.
Prerequisites for Applications Manager

Discussed below are the prerequisites for managing the various monitors:

1. **JBoss**
2. **Tomcat**
3. **WebLogic**
4. **WebSphere**
5. **Custom Websphere Attributes**
6. **PHP**
7. **Apache**
8. **Linux/Solaris**
9. **NTLM Authenticated URLs**
10. **Oracle Applications Server**
11. **Web Transactions Monitor**

**Prerequisites for monitoring JBoss:**

To monitor JBoss, the `http-invoker.sar` should be deployed in the JBoss Server. The application (http-invoker.sar) is by default deployed in the JBoss server.

If the http port of the JBoss server is changed then the port number in the attribute InvokerURLSuffix should also be modified in jboss-3.2.0/server/default/deploy/http-invoker.sar/META-INF/jboss-service.xml file.

**Prerequisites for monitoring Tomcat:**

AdventNet agent has to be deployed in Tomcat Servers 3.x and 4.x. More

In case of Tomcat 5.x, an application named Manager must be running in it for Applications Manager to monitor the Tomcat server. By default, this application will be running in the server. Moreover, the user role to access the server must also be manager. To add a role as “manager” for any of the users such as tomcat, role1, or both, you need to make changes in tomcat-users.xml file located in the /conf directory.

Click the link to view an example tomcat-users.xml, which has user tomcat with role as manager

**Prerequisites for monitoring WebLogic:**

For **WebLogic 6.1**, provide Admin user name.

For monitoring **WebLogic 7.x, 8.x** you should set the `Weblogic.disableMBeanAuthorization` system variable to true for enabling data collection.

Follow the steps given below:

- Edit startWLS.cmd/sh present in the /server/bin directory and add the following argument - `Dweblogic.disableMBeanAuthorization=true` (click on the link to view the sample startWLS.cmd/sh file)
- Restart the WebLogic Server for the changes to take effect

For monitoring **WebLogic 9.x**, you should set the `Weblogic.disableMBeanAuthorization` and `Weblogic.anonymousAdminLookupEnabled` system variables to true for enabling data collection.
Follow the steps given below:

- Edit startWLS.cmdиш present in the /server/bin directory and add the following argument:
  - Dweblogic.disableMBeanAuthorization=true
  - Dweblogic.management.anonymousAdminLookupEnabled=true (click on the link to view the sample startWLS.cmdиш file)
- Restart the WebLogic Server for the changes to take effect

Prerequisites for monitoring WebSphere:

Setting PMI specification level:

By default the Performance Monitoring Infrastructure (PMI) specification level in WebSphere Servers is "None". This has to be changed to "Standard".

Also, the perfServletApp.ear file, which uses the Performance Monitor Interface (PMI) infrastructure to retrieve the performance information from WebSphere Application Server, needs to be installed.

To modify PMI specification level:

- Connect to the Admin console - http://:/admin/
- On the left-side tree expand the Servers node.
- Click on the Applications Servers link. This will display the list of servers running the node.
- Click on the server for which data collection has to be enabled.
- In the Additional Properties table, click on the Performance Monitoring Service.
- Change the Initial specification level to "Standard" and apply the changes. Also enable (select) Startup.

To install perfServletApp.ear:

- In the Admin console, on the left-side tree, click Applications node.
- Click on Enterprise Applications.
- The right-side table lists all the installed applications. Check if perfServletApp is already available. If not, click Install to install the perfServletApp.ear file (which is available by default under the WebSphere installation directory).
- Restart the WebSphere Server.

Prerequisites for monitoring Custom Websphere Attributes:

1. Copy the following jars from <WebSphere installed directory>/lib/ to <Applications Manager Home>/lib/was directory:
   - admin.jar
   - bootstrap.jar
   - ffdc.jar
   - idl.jar
   - iwsorb.jar
   - j2ee.jar
   - jflt.jar
   - jmxc.jar
   - jmxr.jar
   - pmi.jar
   - pmiclient.jar
   - ras.jar
   - sas.jar
2. Copy the following jars from `<WebSphere Installed Directory>/java/jre/lib/ext` to `<Applications Manager Home>/lib/was` directory.
   - soap.jar
   - utils.jar
   - wasjmx.jar
   - wsexception.jar
   - wssec.jar

3. **For Windows and Linux Installation of WebSphere:** Copy the `security.jar` from `<WebSphere installed directory>/java/jre/lib/` to `<Applications Manager Home>/lib/was` directory.
   **For Solaris Installation of WebSphere:** Copy the `ibmjsse.jar` from `<WebSphere Installed Directory>/java/jre/lib/` to `<Applications Manager Home>/lib/was` directory and rename it as `security.jar`

**Prerequisites for monitoring PHP:**

Kindly place the `appmanager.php` file in the webserver's document root. The `appmanager.php` can be found in `<Applications Manager Home>/resources` directory.

**Prerequisites for monitoring Apache:**

Enabling the Server status and the Extended-status will give additional information for the Apache server.

To enable the Server Status, follow the steps given below:

- In Apache's httpd.conf file, locate "Location /server-status" tag.
- Remove the comment in the Location/Server-status tag, to Enable SetHandler server-status.
- Change the attribute "deny from all" to "Allow from all".
- Remove the comment in "LoadModule status_module modules/mod_status.so".
- Save the conf file and restart the Apache Server.

To enable the Extended-status, follow the steps given below:

- Locate "ExtendedStatus" Attribute in httpd.conf file.
- Remove the comment to enable the status.
- Save the conf file and restart the Apache Server.

**Prerequisites for monitoring Linux/Solaris:**

If SSH version is 2.0 and above in your Linux/Solaris servers, for collecting data in SSH mode, a third party SSH Tools are required. Follow the procedure given below to deploy the SSH Tools.

- Download the SSH Tools from `http://prdownloads.sourceforge.net/sshtools/sshtools-j2ssh-0.0.4-alpha-bin.zip`.
- Extract the files from the downloaded.zip file.
- From the extracted files, upload sshtools-j2ssh-0.0.4-alpha.jar and jaxb-rt-1.0-ea.jar files located under directory, to Applications Manager, using the web client's Upload Files/Binaries form.
- Restart the Applications Manager.
• The remote SSH Session could be open sometimes, this is a known issue with the SSH tools, the issue have been fixed and is available as a separate patch. Kindly contact support@appmanager.com to get the patch

This will enable data collection from systems through SSH mode of monitoring (for SSH versions 2.0 and above).

**Prerequisites for monitoring NTLM Authenticated URLs:**

To monitor NTLM authenticated URLs,

• Extract the cryptix-jce-provider.jar from [http://www.cryptix.org/cryptix-jce-20050328-snap.zip](http://www.cryptix.org/cryptix-jce-20050328-snap.zip)
• Copy the files from the cryptix-jce-provider.jar to `<Applications Manager Home>/lib/ext`.
• Restart the Applications Manager.

**Prerequisites for monitoring Oracle Applications Server:**

Applications Manager uses the **Dynamic Monitoring Service (DMS)** provided by Oracle Application Server to monitor the same. For this reason, the DMS Servlet has to be made accessible to the system where the Applications Manager is running.

To enable the access, please follow the instructions provided below
[The instructions are referred from the Oracle website : [http://download-west.oracle.com/docs/cd/B14099_16/core.1012/b14001/monitor.htm#sthref86](http://download-west.oracle.com/docs/cd/B14099_16/core.1012/b14001/monitor.htm#sthref86)]

By default, the dms0/AggreSpy URL is redirected and the redirect location is protected, allowing only the localhost (127.0.0.1) to access the AggreSpy Servlet.

To view metrics from a system other than the localhost you need to change the DMS configuration for the system that is running the Oracle Application Server that you want to monitor by modifying the file `$ORACLE_HOME/Apache/Apache/conf/dms.conf` on UNIX, or `$ORACLE_HOME%Apache%Apache%conf%dms.conf` on Windows systems.

The following example shows a sample default configuration from dms.conf. This configuration limits AggreSpy to access metrics on the localhost (127.0.0.1). The port shown, 7200, may differ on your installation.

**Example:** Sample dms.conf File for localhost Access for DMS Metrics

```
# proxy to DMS AggreSpy

Redirect /dms0/AggreSpy http://localhost:7200/dmsoc4j/AggreSpy

#DMS VirtualHost for access and logging control

Listen 127.0.0.1:7200

OpmnHostPort http://localhost:7200

<VirtualHost 127.0.0.1:7200>

ServerName 127.0.0.1

```

By changing the dms.conf configuration to specify the host that provides, or serves DMS metrics, you can allow users on systems other than the localhost to access the DMS metrics from the location [http://host:port/dms0/AggreSpy](http://host:port/dms0/AggreSpy).
**Caution:** Modifying `dms.conf` has security implications. Only modify this file if you understand the security implications for your site. By exposing metrics to systems other than the localhost, you allow other sites to potentially view critical Oracle Application Server internal status and runtime information.

To view metrics from a system other than the localhost (127.0.0.1), do the following:

- Modify `dms.conf` by changing the entries with the value for localhost "127.0.0.1" shown in Example to the name of the server providing the metrics (obtain the server name from the `ServerName` directive in the `httpd.conf` file, for example `tv.us.oracle.com`).

- Find below a sample updated `dms.conf` that allows access from a system other than the localhost (127.0.0.1).

Example: Sample `dms.conf` File for Remote Host Access for DMS Metrics

```
# proxy to DMS AggreSpy
Redirect /dms0/AggreSpy http://tv.us.oracle.com:7200/dmsoc4j/AggreSpy

# DMS VirtualHost for access and logging control
Listen tv.us.oracle.com:7200
OpmnHostPort http://tv.us.oracle.com:7200
<VirtualHost tv.us.oracle.com:7200>
    ServerName tv.us.oracle.com
</VirtualHost>
```

- Restart, or stop and start the Oracle HTTP Server using Application Server Control Console or using the Oracle Process Manager and Notification Server `opmnctl` command. For example,
  ```
  %opmnctl restartproc process-type=HTTP_Server
  or
  %opmnctl stopproc process-type=HTTP_Server
  %opmnctl startproc process-type=HTTP_Server
  ```

After performing the above steps, please ensure that you are able to access the url `http://<host>:7200/dmsoc4j/AggreSpy` from the Applications Manager system.

**Prerequisites for monitoring Web Transactions:**

Web Transaction Monitor requires an **agent** to be plugged in the application server (like JBoss) to be monitored. Know more about the **Web Transactions Agent**.
Working with Applications Manager

The following are the steps involved in monitoring:

1. **Create a new Monitor Group**: Create a new Monitor Group by grouping one or more Monitors.
2. **Create new Monitor**: Discover Monitors in the network and start collecting data (performance metrics, availability etc) for the same.
3. **Associate Monitor with Monitor Group**: Add the discovered monitors to the Monitor Group.
4. **Create threshold profile**: Create thresholds to identify the status of a specific attribute.
5. **Create actions**: Specify what action needs to be taken in the event of an alert.
6. **Associate threshold and action with the attributes**: Associate the thresholds and action to generate alerts and perform action based on the threshold definition.
7. **Configuring dependencies**: Dependencies specify the rule based on which the severity of health and availability is determined. For example, Health of a Tomcat Server may depend on the overall response time of the server or on the response time of each of the web applications deployed on the server etc. By configuring dependencies, you can determine the attribute, based on which the severity of health changes.

You can either perform the above tasks individually or using a wizard. For more information on using the wizard to perform all the above mentioned tasks, refer to Using Monitor Group Wizard topic.

Please go through Working with Monitor Group and Configuring Alerts for detailed information on the above.
Working with Monitor Groups

Monitor Groups are a logical group of one or more Monitors that provides a holistic view of your business environment.

For example, the health of an online Web application depends on various factors, such as the health of the application server hosting the Web application, the availability of the Web server for accessing the Web applications, the database server for storing or getting the required information, etc. These web applications and services can be grouped together and monitored as a single Monitor Group.

Troubleshoot: For any monitoring-related troubleshooting, refer to the online Troubleshooting section.

The following sections are the steps involved to work with a Monitor Group:

- Using Monitor Group Wizard
- Creating New Monitor Group
- Creating New Monitor
- Associating Monitor with Monitor Groups
- Deleting Monitor from Monitor Groups
- Deleting a Monitor Group
Using Monitor Group Wizard

This section explains how you can create a new Monitor Group using a Wizard. This wizard helps you in not only creating a new Monitor Group, but also helps you in associating existing Monitors to this Group and also configuring for Alerts.

To create a new Monitor Group using Monitor Group Wizard

1. Click **New Monitor Group**. The **New Monitor Group Wizard** is displayed.
2. Provide a **Name** for the Monitor Group. This is mandatory and only alphanumeric characters, dashes (-), underscores (_), periods (.), and spaces ( ) are allowed.
3. Provide **Description**, if required.
4. Select the **Owners** from the list of users created. Refer **User Administration** topic for more information on the different roles of users. **Note:** Irrespective of the owners assigned to a monitor group, the monitor group will be visible to all types of users except the operators.
5. Select the **location** for associating the monitor group to **Google Map Business View**. Else by clicking on 'Add Location', google map opens up. Here you can select and and custom locations.
6. Click **Finish** to create the Monitor Group and to add Monitors later. Click **Next** to associate existing Monitors to the Monitor Group.
7. A list of Monitor Types is displayed in the next page. Select the Monitor Type.
8. Click **Finish** to end the wizard or click **Next** to configure Alerts. If you are finishing the wizard, you will be taken to the Monitor Group page. Selecting Next will take you the screen where you can add a new Monitor for the selected Monitor Type.
9. In the next screen, specify the Monitor details. Click **Create** to add and associate the Monitor to the Monitor Group and go to Configure Alert page (refer next step) of the wizard. Click **Create and Add More..** to associate that Monitor and add more Monitors. Click **Finish** to go the Monitor Group page without adding or associating the Monitor.
10. The fourth page in the wizard is to configure Alerts for the Monitors. This page displays all the Monitors associated with that Monitor Group where you can configure Alerts and Thresholds.
11. Click **Finish** to complete the wizard. On completing, you will be taken to the Monitor Group home page that you have just created.
Creating New Monitor Group

This section explains how you can create a new Monitor Group. A monitor Group is particularly useful for grouping the resources of a location say the resources available in sales office or for grouping the resources used by a business application.

To create a new Monitor Group, follow the steps given below:

1. Click **New Monitor Group**.
2. Provide a **Name** for the Monitor Group. This is mandatory and only alphanumeric characters, dashes (-), underscores (_), periods (.), and spaces ( ) are allowed.
3. Provide any **Description**, if required.
4. Under Advanced Options, Select the **Owner** from the list of users created. Refer User Administration topic for more information on the different roles of users.  
   **Note:** Irrespective of the owners assigned to a monitor group, the monitor group will be visible to all types of users except the operators.
5. Select the **location** for associating the monitor group to Google Map Business View. Else by clicking on 'Add Location', google map opens up. Here you can add and select custom locations.
6. Click **Finish** to create the Monitor Group and to add Monitors later.
Associating Monitor with Monitor Groups

To associate Monitor to a Monitor Group, follow the given steps below:

1. Click on the Monitor Group (from Home tab).

2. Under Monitor Group Information, click Associate Monitors link. Alternatively, select the Monitor Type by moving the mouse over the Associate Monitor of Monitor Group Links in the left frame.

3. A list of discovered Monitors that are available for associating and those that have already been associated with that Monitor Group is displayed.

4. Select the check box of the corresponding Monitor from Monitors not present in this Monitor Group list and click Add. You can also remove a Monitor which has already been associated with the Monitor Group by selecting the check box of Monitor(s) under Monitors present in this Monitor Group and clicking Remove.
Deleting Monitor from Monitor Groups

To delete a Monitor from a Monitor Group,
1. Click the Home module tab to display the list of Monitor Groups created.
2. Click the Monitor Group from which the Monitor has to be deleted.
3. Data of all Monitors in that Monitor Group is displayed graphically. Click Remove from Group.

This deletes the Monitor only from the Monitor Group but its monitoring will not stop.

Deleting Monitor from Applications Manager

To delete a Monitor from getting monitored by Applications Manager itself, follow the given steps:
1. Click the Monitor module tab.
2. From Select View combo box, select Monitors View - All. All the Monitor Types are listed.
3. Select the check box of the Monitor and click Delete.
Deleting a Monitor Group

To delete a Monitor Group,

1. Click the **Home** module tab to display the list of Monitor Groups created.
2. Click the Monitor Group to be deleted.
3. On the Left-side **Monitor Group Links**, click **Delete**.

**Note:** However, the Monitor pertaining to the corresponding Monitor Group will not be deleted. You will still be able to view the details of the Monitor that was associated with the Monitor Group. To delete the Monitor, refer to the [Deleting Monitor from Applications Manager](#) section.
Creating New Monitor

Once a new Monitor Group is created, the Monitors such as WebLogic Server, JBoss Server, Tomcat Server, WebSphere Server, MySQL DB Server, Oracle DB Server, Mail Server, etc. must be created. This discovers the Monitor from the network and start collecting data for monitoring.

You have to create a Monitor to discover it from the network and monitor it. This can be done by following the options given below:

- All Monitors in a host.
- A specific Monitor in a host.
- All Monitors in a network- Refer to Discover Network of Performing Admin Activities.

All Monitors in a Host

To discover all Monitors running on a host, create them using the All Monitors option. Follow the given steps for discovering the Monitor:

1. Select New Monitor.
2. Choose All Services from the Add Monitor of type combo box.
3. Provide the hostname, where all the Monitors running on this host will be discovered. You can also discover monitors in multiple hosts by providing the hostname, separated by commas.
   
   Note: This will start discovering in the default port of the Monitor.
4. Enter the SubNetMask of the network.
5. Click Add Monitor(s).

A Specific Monitor in a host

To discover a specific Monitor in a host, create them by referring to the following sections:

- Application Servers
- Web Transactions Monitoring
- Database Servers
- Servers
- Mail Servers
- Services
- Web Services
- URL Monitoring
- JMX / SNMP Dashboard
- Script Monitoring
- QEngine Script Monitoring
Application Servers

The Application servers are designed to develop Web services and Web applications. Failure in diagnosing any problem in these services/applications results in poor productivity and performance.

Applications Manager monitors these servers and applications to detect such problems affecting the business process management.

The following are the different Application Servers supported by Applications Manager:

- Microsoft .NET
- JBoss Server
- Oracle Application Server
- Tomcat Server
- WebLogic Server
- WebSphere Server

**Microsoft .NET**

To create Microsoft .NET Monitor

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **Microsoft .NET Monitor**.
3. Enter the **IP Address** or **hostname** of the host where .NET runs.
4. Enter the **SubNetMask** of the network.
5. Set the **Polling Interval**.
6. Enter the **User Name** and **Password** of the system.
7. Choose the **Monitor Group** from the combo box with which you want to associate .NET Monitor (optional).
8. Click **Add Monitor(s)**. This discovers .NET from the network and starts monitoring them.

**JBoss Server**

Supported versions of JBoss Server: 3.2.x, 4.0.1, 4.0.2, 4.0.3

For help in monitoring other versions of JBoss 4.x, contact support@appmanager.com.

For Applications Manager to monitor JBoss, it should be able to access the host where JBoss server runs and vice versa. For more information, refer to online Troubleshooting section.

**Prerequisite:** To monitor JBoss, the **http-invoker.sar** should be deployed in the JBoss Server. Know more in the **Prerequisite section**.

To create a JBoss Server Monitor

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **JBoss**.
3. Enter the **IP Address** or **hostname** of the host where JBoss runs.
4. Enter the **SubNetMask** of the network.
5. Enter the **port number** for eg., 8080.
6. Choose **SSL option**, if SSL is enabled in JBoss server.
7. Choose the **JBoss version**.
8. Set the **Polling Interval**.
9. Choose if you want to enable **Web Transactions**.
10. Enter the **User Name** and **Password**, if JBoss has authentication information.
11. Choose the **Monitor Group** from the combo box with which you want to associate JBoss Server Monitor (optional).
12. Click **Add Monitor(s)**. This discovers JBoss server from the network and starts monitoring them.

**Troubleshoot:** Having trouble in monitoring JBoss server? Refer to the [online troubleshooting section](#).

### Oracle Application Server

Supported version of Oracle Application Server: 10g

Applications Manager uses the **Dynamic Monitoring Service (DMS)** provided by Oracle Application Server to monitor the same. For this reason, the DMS Servlet has to be made accessible to the system where the Applications Manager is running. Refer [Prerequisites Section](#).

**To create a Oracle Application Server Monitor**

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **Oracle AS**.
3. Enter the **IP Address** or **hostname** of the host where Oracle Application Server runs.
4. Enter the **SubNetMask** of the network.
5. Enter the **Port number** for eg., 7200.
6. Choose the **Monitor Group** from the combo box with which, you want to associate Oracle Application Server Monitor (optional).
7. Click **Add Monitor(s)**. This discovers Oracle Application Server from the network and starts monitoring them.

### Tomcat Server

The supported versions of Tomcat Servers are 3.x, 4.x, and 5.x. **For Tomcat Server 3.x and 4.x, agent has to be deployed for monitoring.**

**Note:** You can check whether the Agent is deployed, by connecting to the following URL in Tomcat Server.

```
http://<Tomcat-Host>:<Tomcat-Port>/adventnet/DataServlet
```

**To deploy the agent for Tomcat Server 3.x**

1. Download the **Tomcat3Agent.Zip** from `<Applications Manager Home>/working/classes` directory.
2. Unzip it in the `<Tomcat Home>` directory of the host in which the Tomcat server is running.
3. Restart the Tomcat Server.

**To deploy the agent for Tomcat Server 4.x**

1. Download the **Tomcat4Agent.Zip** from the `<Applications Manager Home>/working/classes` directory
2. Unzip it in the `<Tomcat Home>` directory of the host in which the Tomcat server is running.
3. Add the following tag in `server.xml` file located in the `<Tomcat Home>/conf` directory (below the Engine tag).

```xml
<Valve
    className="com.adventnet.appmanager.tomcatagent.ver4.valve.AdventNetHostValve"/>
```

[Click the link to view an example server.xml]

4. Restart the Tomcat Server.

### To deploy the agent for Tomcat Server 4.x and Apache server combined

1. Download the `Tomcat4Agent.Zip` from the `<Applications Manager Home>/working/classes` directory
2. Unzip it in the `<Tomcat Home>` directory of the host in which the Tomcat server is running.
3. Add the following tag in `server.xml` file located in the `<Tomcat Home>/conf` directory (below the Engine tag).

```xml
<Valve
    className="com.adventnet.appmanager.tomcatagent.ver4.valve.AdventNetHostValve"/>
```

[Click the link to view an example server.xml]

4. Restart the Tomcat Server.

5. **Apache:**

   In `Apache mod_jk.conf` file of Apache Server, add the following entry

   ```
   JkMount /adventnet/* ajp13,
   Where ajp13 is the worker name. It has be the name given in `worker.properties` file.
   ```

6. Restart Apache server

### To create a Tomcat Server Monitor

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **Tomcat Server**.
3. Enter the **IP Address** or **hostname** of the host. [Note: Also refer to Configurations based on Tomcat Deployments section]
4. Enter the **SubNetMask** of the network.
5. Enter the **port number** in which the monitor is running. [Default port number is 8080]
6. Choose **SSL option**, if SSL is enabled in Tomcat server.
7. Enter the **polling interval** time in minutes.
8. Provide the monitor-specific authentication information, such as user name and password.

**Note:** Tomcat 3.x and 4.x needs no user name and password. In case of Tomcat 5.x, an application named **Manager** must be running in it for Applications Manager to monitor the Tomcat server. By default, this application will be running in the server. Moreover, the user role to access the server must also be **manager**.

To add a role as "manager" for any of the users such as tomcat, role1, or both, you need make changes in `tomcat-users.xml` file located in the `<TOMCAT-HOME>/conf` directory.

**Example:**

Default configurations in `tomcat-users.xml` in Tomcat Server.
<tomcat-users>
  <user name="tomcat" password="tomcat" roles="tomcat" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>

After adding the roles for the "tomcat" user, the modified entries will be as follows:

<tomcat-users>
  <user name="tomcat" password="tomcat" roles="tomcat,manager" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>

On making the configuration, restart the Tomcat Server.

Now, when adding a new Tomcat (5.x) monitor, specify the username/password as tomcat/tomcat when discovering the Tomcat Server.

[Click the link to view an example tomcat-users.xml]

8. Choose the Monitor Group from the combo box with which you want to associate Tomcat Server Monitor (optional).

9. Click Add Monitor(s). This discovers Tomcat server from the network and starts monitoring them.

Troubleshoot: Having trouble in monitoring Tomcat server? Refer to the online Troubleshooting section.

Note : Steps to configure Tomcat Monitor for JBoss 3.2.5

1. Append the following in the web.xml present in
   <JBOSSE_SERVER_HOME>\deploy\jbossweb-tomcat50.sar\ROOT.war\WEB-INF folder

   " <servlet-mapping>
   <servlet-name>Status Servlet</servlet-name>
   <url-pattern>/manager/status</url-pattern>
   </servlet-mapping>
   <servlet-mapping>
   <servlet-name>Status Servlet</servlet-name>
   <url-pattern>/manager/</url-pattern>
   </servlet-mapping>
   <servlet-mapping>
   <servlet-name>Status Servlet</servlet-name>
   <url-pattern>/manager/status/</url-pattern>
   </servlet-mapping>
   <servlet-mapping>
   <servlet-name>Status Servlet</servlet-name>
   <url-pattern>/manager/status/</url-pattern>
   </servlet-mapping> "

AdventNet ManageEngine Applications Manager – Help Documentation

AdventNet, Inc.
2. Restart the JBoss server.
3. Configure a tomcat monitor by clicking New Monitor --> Select Tomcat Server in the combo box.
4. Select the version as 5.x and create the monitor. This will create a monitor for the Tomcat webserver running in JBoss3.2.5.

Configurations based on Tomcat Server Deployment

Monitoring of Tomcat Server depends on its deployment. This section explains the possible deployment scenarios of Tomcat. Your configuration of host name and the port depends on these scenarios.

1. Standalone Tomcat Server

This is a general scenario wherein you have a Tomcat server which has the HTTP (apache) within its deployment. In this case, when configuring a tomcat monitor, specify the host name of the Tomcat server and the port of the HTTP.

Example: Tomcat server name: Tomcat A; HTTP (in Tomcat server) port: 8080; External Apache server port: 80

In this case, while configuring for a Tomcat monitor, specify the host name as ‘Tomcat A’ and specify the port of the HTTP that runs with the Tomcat and not the external Apache, i.e., specify the port as 8080 and not 80.

2. One Tomcat Server (with HTTP) and one external instance of Apache

There is one Tomcat server with HTTP (apache) instance running in it and another external Apache running outside.

Example: Tomcat server name: Tomcat A; HTTP (in Tomcat server) port: Not available; External Apache server port: 80

In this case, while configuring for a Tomcat monitor, specify the host name as ‘Tomcat A’ and specify the port of the external Apache, i.e., 80.

3. One Tomcat Server (without HTTP) and one external instance of Apache

There is one Tomcat server without HTTP in it and another external Apache running.

Example: Tomcat server name: Tomcat A; HTTP (in Tomcat server) port: Not available; External Apache server port: 80

In this case, while configuring for a Tomcat monitor, specify the host name as ‘Tomcat A’ and specify the port of the external Apache, i.e., 80.

4. Multiple Tomcat Server (with HTTP instances in each of these servers) and one external instance of Apache

There are multiple Tomcat servers, say 3, with HTTP instances in each of them and another external Apache running.

Example: Tomcat Server names: Tomcat A, Tomcat B, Tomcat C; HTTP (in Tomcat servers) port: 8070, 8080, 8090 respectively; External Apache server port: 80

In this case, you need to create tomcat server monitor individually for Tomcat A, Tomcat B, and Tomcat C and specify their ports as 8070, 8080, and 8090 respectively.
5. Multiple Tomcat Server (without HTTP instances in these servers) and one external instance of Apache

There are multiple Tomcat servers, say 3, without HTTP instances in them and another external Apache running.

**Example:** Tomcat Server names: Tomcat A, Tomcat B, Tomcat C; HTTP (in Tomcat servers) port: Not available; External Apache server port: 80

You can monitor only one of the instances in this case. Please contact support@appmanager.com if you would like to have it added.

### WebLogic Server

The supported versions of WebLogic Servers are 6.1, 7.x, 8.x, 9.0, 9.1.

Know the **Prerequisites** that are required to monitor WebLogic.

#### To create a WebLogic Server Monitor

1. Click the **New Monitor**.
2. From Add Monitor of type combo box, select **WebLogic Server**.
3. Enter the **IP Address/ hostname** of the host.
4. Enter the **SubNetMask** of the network.
5. Enter the **port number** in which WebLogic is running.
6. Enter the **polling interval** time in minutes.
7. Provide the monitor-specific authentication information, such as **username and password**.

**Note:** WebLogic Server needs some additional configuration and conditions to be followed for monitoring.

- For **WebLogic 6.1**, provide only Admin user name.
- For monitoring **WebLogic 7.x, 8.x**, you should set the `weblogic.disableMBeanAuthorization` system variable to **true** for enabling data collection. Follow the steps given below:
  1. Edit `startWLS.cmdsh` present in the `<WLS_HOME>/server/bin` directory and add the following argument `weblogic.disableMBeanAuthorization=true` (click on the link to view the sample `startWLS.cmdsh` file).
  2. Restart the WebLogic Server for the changes to take effect.
- For monitoring **WebLogic 9.x**, you should set the `weblogic.disableMBeanAuthorization` and `Weblogic.anonymousAdminLookupEnabled` system variables to true for enabling data collection. Follow the steps given below:
  1. Edit `startWLS.cmdsh` present in the `/server/bin` directory and add the following argument
     `-Dweblogic.disableMBeanAuthorization=true -Dweblogic.management.anonymousAdminLookupEnabled=true` (click on the link to view the sample `startWLS.cmdsh` file).
  2. Restart the WebLogic Server for the changes to take effect.

8. Choose the **Monitor Group** from the combo box with which you want to associate WebLogic Server Monitor (optional).
9. Click **Add Monitor(s)**. This discovers WebLogic server from the network and starts monitoring them.
Troubleshoot: Having trouble in monitoring WebLogic server? Refer to the online Troubleshooting section.

WebSphere Server

The supported versions of WebSphere Servers are 5.x and 6.x. For Applications Manager to collect data from WebSphere, configurations are required at the Performance Monitoring Infrastructure (PMI) specification level. Refer Prerequisites Section

To create a WebSphere Server Monitor

1. Click the New Monitor.
2. From Add Monitor of type combo box, select WebSphere Server.
3. Select the Deployment Mode as Base or Network Deployment.
4. For Base Mode, Enter the Host name/IP Address of the host. For Network Deployment, enter the Host name/IP Address of any one of the WebSphere servers and not the Network Deployer's. This will automatically discover all the WebSphere servers in Network Deployment.
5. Enter the SubNetMask of the network.
6. Enter the HTTP Transport Port (9080 by default).
7. Enter the polling interval time in minutes.
8. Select the version of the WebSphere to be monitored - 5.x or 6.x.
9. Enter the port number of the SOAP Connector (8880 by default). SOAP connector establishes connection between the Applications Manager and the WebSphere server. This is required only for Custom JMX MBeans Monitoring.
10. Enter the User Name and Password, if Global Security is enabled.
11. In Network Deployment Mode, Enter the Network Deployer's Host and SOAP Port (Default : 8879). Custom Attributes would be added using this information.
12. Choose the Monitor Group from the combo box with which you want to associate WebSphere Server Monitor (optional).
13. Click Add Monitor(s). This discovers WebSphere server from the network and starts monitoring them.

Troubleshoot: Having trouble in monitoring WebSphere server? Refer to the online Troubleshooting section.

Note: To add Custom WebSphere Attributes, refer Custom Monitors.

Configuration in WebSphere - Setting PMI specification level

By default the Performance Monitoring Infrastructure (PMI) specification level in WebSphere Servers is "None". This has to be changed to "Standard". Also, the perfServletApp.ear file which uses the Performance Monitor Interface (PMI) infrastructure to retrieve the performance information from WebSphere Application Server needs to be installed.

If you have already made these configurations, you can ignore this section.

To modify PMI specification level

1. Connect to the Admin console - http://<Host>:<Port>/admin/
2. On the left-side tree expand the Servers node.
3. Click on the Applications Servers link. This will display the list of servers running the node.
4. Click on the server for which data collection has to be enabled.
5. In WebSphere 5.x, Go to the **Additional Properties** table, click on the **Performance Monitoring Service**. Change the Initial specification level to "Standard" and **Apply** the changes. Also enable (select) **Startup**
6. In WebSphere 6.x, Click on **Performance Monitoring Infrastructure** link. Then enable PMI and select "all" for **Currently Monitored Statistics Set**. Apply the changes.

**To install perfServletApp.ear**

1. In the Admin console, on the left-side tree, click **Applications** node.
2. Click on **Enterprise Applications**.
3. The right-side table lists all the installed applications. Check if perfServletApp is already available. If not, click **Install** to install the **perfServletApp.ear** file (which is available by default under the `<WebSphere Installed Location>/WebSphere/AppServer/InstallableApps` directory, Example: `C:/Program Files/WebSphere/AppServer/InstallableApps/perfServletApp.ear`).

After performing these above configurations, restart the WebSphere Server.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

**See Also**

Monitor Information - Application Servers | Create Other New Monitors
Database Servers

Database servers are robust, enterprise-class database management system. Applications Manager provides Database Server monitoring that monitors database resources. This database server monitoring involves connecting to the database resource, collecting data, and representing its attribute details as graphs.

The following are the different Database servers supported by Applications Manager:

- MySQL Database Server
- Oracle Database Server
- MS SQL Database Server
- IBM DB2 Database Server

MySQL Database Server

To create a MySQL database server Monitor, follow the given steps:

1. Click the New Monitor.
2. From Add Monitor of type combo box, select MySQL DB Server.
3. Enter the IP Address or hostname of the host.
4. Enter the SubNetMask of the network.
5. Enter the port number in which MySQL is running.
6. Enter the polling interval time in minutes.
7. Provide the user name and password of user who has permission to access the MySQL database.
8. Specify the database name. Please note that the Database name must be valid. Also, the database name is associated with the user name. Hence, provide the database name corresponding to the user name given in the above field.
9. Choose the Monitor Group from the combo box with which you want to associate MySQL database server Monitor (optional).
10. Click Add Monitor(s). This discovers MySQL database server from the network and starts monitoring them.

**Note:** In the MySQL database (that you are trying to monitor), ensure that the user name assigned to Applications Manager has the permission to access the MySQL database from the host where Applications Manager is running. Else, give a relevant user who has the privileges to do the same.

Troubleshoot: Having trouble in monitoring MySQL database server? Refer to the online Troubleshooting section.

Oracle Database Server

Follow the given steps to create a Oracle database server Monitor:

1. Click the New Monitor.
2. From Add Monitor of type combo box, select Oracle DB Server.
3. Enter the IP Address or hostname of the host.
4. Enter the SubNetMask of the network.
5. Enter the port number in which the Oracle is running.
6. Enter the **polling interval** time in minutes.
7. Provide the **user name** of the admin user ('system' is the default username) and its corresponding password.
8. Provide a valid **Database name**.
9. Choose the **Monitor Group** from the combo box with which you want to associate Oracle database server Monitor (optional).
10. Click **Add Monitor(s)**. This discovers Oracle database server from the network and starts monitoring them.

**Troubleshoot:** Having trouble in monitoring Oracle database server? Refer to the online Troubleshooting section.

### MS SQL Database Server

To create a MS SQL database server Monitor, follow the given steps:

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **MS SQL DB Server**.
3. Enter the **IP Address** or **hostname** of the host.
4. Enter the **SubNetMask** of the network.
5. Enter the **port number** in which the MS SQL is running.
6. Enter the **polling interval** time in minutes.
7. Provide the **user name** and **password** of user who has permission to access the MS SQL database. The user name specified for collecting the data from MS SQL Server should have either System Administrator role or the user should be the DB owner for master database.
8. Specify the **database name**.
9. Choose the **Monitor Group** from the combo box with which you want to associate MS SQL database server Monitor (optional).
10. Click **Add Monitor(s)**. This discovers MS SQL database server from the network and starts monitoring them.

**Troubleshoot:** Having trouble in monitoring MS SQL database server? Refer to the online Troubleshooting section.

### IBM DB2 Database Server

To create a IBM DB2 database server Monitor, follow the given steps:

1. Click the **New Monitor**.
2. From **Add Monitor of type** combo box, select **DB2 DB Server**.
3. Enter the **IP Address** or **hostname** of the host.
4. Enter the **SubNetMask** of the network.
5. Enter the **port number** in which the is running.
6. Enter the **polling interval** time in minutes.
7. Provide the **user name** and **password** of user who has permission to access the DB2 database. The user name specified for collecting the data from DB2 Server should have either System Administrator role or the user should be the DB owner for master database.
8. Specify the **database name**.

9. Choose the **Monitor Group** from the combo box with which you want to associate MS SQL database server Monitor (optional).

10. Click **Add Monitor(s)**. This discovers DB2 database server from the network and starts monitoring them.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

**See Also**

Monitor Information - Database Server | Create Other New Monitors
Services

Applications Manager supports monitoring of the following services to check their status:

- JMX [MX4J / JDK 1.5]
- Service Monitoring
- AdventNet JMX Agent - RMI Adapter
- SNMP
- Telnet

JMX [MX4J / JDK 1.5]

To create a MX4J RMI Connector Monitor, follow the given steps:

1. Click **New Monitor**. From the combo box, choose **JMX [MX4J / JDK 1.5]**.
2. Enter the **IP Address or hostname** of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which RMI Adapter is running. Also, you can provide multiple ports separated by commas.
5. Enter the **polling interval** time in minutes.
6. Enter the **JNDI name**. For example, `/jmxconnector`.
7. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
8. Click **Add Monitor(s)**. This discovers the **Monitor** from the network and starts monitoring them.

Service Monitoring

To create a Service Monitoring Monitor, follow the steps given below:

1. Click the **New Monitor**. From the combo box, choose **Service Monitoring**.
2. Enter the **IP Address or hostname** in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Enter the **port number** in which the service you want to monitor is running.
5. Enter the **polling interval** time in minutes.
6. Enter the **command** that will be executed after connecting to the port mentioned above. For example, if the port added is where your web server is running, then you can give the command as `GET / HTTP/1.0`. This will get the index page of the web server.
7. Enter the **string** that has to be searched after executing the command.
8. Choose the **Monitor Group** from the combo box with which you want to associate Service Monitoring Monitor (optional).
9. Click **Add Monitor(s)**. This discovers the Service and starts monitoring them.

AdventNet JMX Agent - RMI Adapter

To create a JMX Agent - RMI Adapter Monitor, follow the steps given below:

1. Click the **New Monitor**. From the combo box, choose **AdventNet JMX Agent - RMI Adapter**.
2. Enter the **IP Address or hostname** of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which the RMI adapter is running in the host.
5. Enter the **polling interval** time in minutes.
6. Choose the **Monitor Group** from the combo box with which you want to associate JMX Agent Monitor (optional).
7. Click **Add Monitor(s)**. This discovers the RMI adapter in the host and starts monitoring them.

**SNMP (v1 or v2c)**

To create a SNMP Monitor, follow the steps given below:

1. Click the **New Monitor**. From the combo box, choose **SNMP (V1 or V2c)**.
2. Enter the **IP Address or hostname** of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which SNMP is running in the host (default port number is 161).
5. Enter the **polling interval** time in minutes.
6. Enter the **timeout** value in seconds.
7. Enter the **Community String** (‘public’ by default).
8. Choose the **Monitor Group** from the combo box with which you want to associate SNMP Monitor (optional).
9. Click **Add Monitor(s)**. This discovers SNMP in the host and starts monitoring them.

**Telnet**

To create a Telnet Monitor, follow the steps given below:

1. Click the **New Monitor**. From the combo box, choose **Telnet**.
2. Enter the **IP Address or hostname** of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which the monitor is running.
5. Enter the **polling interval** time in minutes.
6. Choose the **Monitor Group** from the combo box with which you want to associate Telnet Monitor (optional).
7. Click **Add Monitor(s)**. This discovers the telnet from the network and starts monitoring them.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

**See Also**

Monitor Information - Services | Create Other New Monitors
Mail Servers

Applications Manager supports monitoring of the following Mail Servers:

- Exchange Server
- Mail Server

Exchange Server

To create a Exchange Server Monitor, follow the given steps:

1. Click New Monitor. From the combo box, choose Exchange Server.
2. Enter the IP Address or hostname of the host in which the Exchange Server is running.
3. Enter the SubNetMask of the network.
4. Provide the port number in which Exchange Server is running. Also, you can provide multiple ports separated by commas.
5. Enter the polling interval time in minutes.
7. Select Exchange Server Services
   - MS Exchange Information Store
   - MS Exchange Site Replication Store
   - MS Exchange MTA Stacks
   - MS Exchange Management
   - SMTP
   - POP3
   - IMAP4
   - MS Exchange System Attendant
   - MS Exchange Routing Engine
   - MS Exchange Event Service
8. Provide the authentication details User Name and Password for the system in which Exchange server is running.
9. Choose the Monitor Group from the combo box to which you want to associate the Monitor (optional).
10. Click Add Monitor(s). This discovers the Monitor from the network and starts monitoring them.

   **Note:** Only if Applications Manager is running in Windows System, monitoring of Exchange Server is possible.

Mail Server

To create a Mail Server Monitor, follow the steps given below:

1. Click the New Monitor. From the combo box, choose Mail Server.
2. Enter the IP Address or hostname of the host in which the SMTP server is running.
3. Enter the SubNetMask of the network.
4. Enter the SMTP Port number.
5. Enter an Email ID available in that SMTP server.
6. If the SMTP server requires authentication, specify the User Name and Password by clicking SMTP Server requires Authentication field.
7. If the POP/Imap service is in a different host, specify its **POP/Imap Host** (host where POP service runs) and **POP Port**. Also provide the authentication details **User Name** and **Password** for the POP service. If the SMTP and POP/Imap service are running in the same host, then ignore this step.

8. Enter the **message** to appear in the subject of the mail.

9. Enter the **polling interval** time in minutes, in **Polling Interval** field.

10. Choose the **Monitor Group** from the combo box with which you want to associate Mail Server Monitor (optional).

11. Click **Add Monitor(s)**. This discovers the Mail server from the network and starts monitoring them.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

**See Also**

Monitor Information - Mail Servers | Create Other New Monitors
Web Services

Applications Manager supports monitoring of the following Web Services to check their status:

- Apache Server
- IIS Server
- PHP
- Web Server
- HTTP - URLs and HTTP - URL Sequence

Apache Server

To create an Apache Monitor, follow the steps given below: Refer to the Prerequisites that are needed for Apache monitoring.

1. Click the New Monitor. From the combo box, choose Apache Server.
2. Enter the IP Address or hostname of the host in which the Monitor is running.
3. Enter the SubNetMask of the network.
4. Provide the port number in which the monitor is running.
5. Choose SSL option, if SSL is enabled in Apache Server.
6. Enter the polling interval time in minutes.
7. Choose the Monitor Group from the combo box with which you want to associate Apache Monitor (optional).
8. Click Add Monitor(s). This discovers the Apache from the network and starts monitoring them.

IIS Server

To create an IIS Monitor, follow the steps given below:

1. Click the New Monitor. From the combo box, choose IIS Server.
2. Enter the IP Address or hostname of the host in which the Monitor is running.
3. Enter the SubNetMask of the network.
4. Provide the port number in which the monitor is running.
5. Choose SSL option, if SSL is enabled in IIS Server.
6. Enter the polling interval time in minutes.
7. Choose the Monitor Group from the combo box with which you want to associate IIS Monitor (optional).
8. Click Add Monitor(s). This discovers the IIS Server from the network and starts monitoring them.

PHP

To create a PHP Monitor, follow the steps given below:

Initially, you need to place appmanager.php, the bundled Applications Manager's PHP file in the webserver's document root.

1. Click on New Monitor. From the combo box, select PHP Monitoring.
2. Enter the IP Address or hostname of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which the monitor is running.
5. Choose **SSL** option, if SSL is enabled in PHP.
6. Enter the **path** to be connected. By default, '/appmanager.php' is shown. http://hostname:portNo/'path to be connected" will be used for connection
7. Enter the **polling interval** time in minutes.
8. Choose the **Monitor Group** from the combo box with which you want to associate PHP Monitor (optional).
9. Click **Add Monitor(s)**. This discovers the PHP Service from the network and starts monitoring them.

**Web Server**

To create a Web Server Monitor, follow the steps given below:

1. Click the **New Monitor**. From the combo box, choose **Web Server**.
2. Enter the **IP Address or hostname** of the host in which the Monitor is running.
3. Enter the **SubNetMask** of the network.
4. Provide the **port number** in which the monitor is running.
5. Enter the **polling interval** time in minutes.
6. Choose the **Monitor Group** from the combo box with which you want to associate Web Server Monitor (optional).
7. Click **Add Monitor(s)**. This discovers the Web server from the network and starts monitoring them.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

**See Also**

Monitor Information - Web Services | Create Other New Monitors
Servers

Server level management is a concept which involves lot of manual intervention, human resources, and administrative tasks to be performed. Applications Manager provides with a Server level monitoring functionality to achieve such goals and to ease the process of configuration management of hosts.

The different type of servers that are supported by Applications Manager are:
- Windows 2000, 2003, XP, NT
- Linux
- Sun OS
- IBM AIX
- HP Unix
- Tru64 Unix
- FreeBSD

To create the above server Monitor, follow the given steps:
1. Click New Monitor. From the combo box, choose Server.
2. Enter the IP Address or hostname of the host.
3. Enter the SubNetMask of the network.
4. Enter the polling interval time in minutes.
5. Provide the monitor specific authentication information: Choose the OS type (FreeBSD, AIX, Linux, HP UX, Sun OS, Windows 2000, 2003, XP, NT). Based on the type of OS, the Mode of Monitoring information changes.

**Windows 2000/2003/XP/NT:**
1. Select the Mode of Monitoring (SNMP or WMI).
2. If SNMP, provide the port at which it is running (default is 161) and SNMP Community String (default is 'public'). This requires no user name and password information.
3. If WMI, provide user name and password information of the server.

**Linux/ Sun OS/ IBM AIX/ HP Unix/Tru64 Unix/FreeBSD:**
4. Select the Mode of Monitoring (Telnet, SSH or SNMP). For IBM AIX, HP Unix, Tru64 Unix, only Telnet and SSH are supported
5. If Telnet, provide the port number (default is 23) and user name and password information of the server.
6. If SSH, provide the port number (default is 22) and user name and password information of the server.
7. If SNMP, provide the port at which it is running (default is 161) and SNMP Community String (default is 'public'). This requires no user name and password information.

For Telnet/SSH mode of monitoring, specify the command prompt value, which is the last character in your command prompt. Default value is $ and possible values are >, #, etc.

**Note:** In the server which you are trying to monitor through SSH, the PasswordAuthentication variable should be set as 'yes' for the data collection to happen. To ensure this, access the file /etc/ssh/sshd_config and verify the value of PasswordAuthentication variable. If it is set as 'no', modify it to 'yes' and restart the SSH Daemon using the command /etc/rc.d/sshd restart.
**Note:** If SSH version is 2.0 and above in your Linux/Solaris servers, for collecting data in SSH mode, a third party tool **SSH Tools** is required. Follow the procedure given below to deploy the SSH Tools.

i) Download the SSH Tools from [http://prdownloads.sourceforge.net/sshtools/sshtools-j2ssh-0.0.4-alpha-bin.zip](http://prdownloads.sourceforge.net/sshtools/sshtools-j2ssh-0.0.4-alpha-bin.zip)

ii) Extract the files from the downloaded .zip file.

iii) From the extracted files, upload `sshtools-j2ssh-0.0.4-alpha.jar` and `jaxb-rt-1.0-ea.jar` files located under `<lib>` directory, to Applications Manager, using the web client's **Upload Files/Binaries** form.

iv) Restart the Applications Manager.

This will enable data collection from servers through SSH mode of monitoring (for SSH versions 2.0 and above).

**Note:** The remote SSH Session could be open sometimes, this is a known issue with the SSH tools, the issue have been fixed and is available as a separate patch. Kindly contact support@appmanager.com to get the patch.

6. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).

7. Click **Add Monitor(s)**. This discovers the host or server from the network and starts monitoring them.

If you have added Monitors and not associated them with a Monitor Group, you can do this manually anytime. For information on associating a Monitor with a Monitor Group, refer to **Associating Monitor with Monitor Groups** topic.

There are situations, where the host gets automatically discovered with the Monitor running in the host. To disable the default option, disable it using **Global Settings**.

It is important to note that if Applications Manager server is running in Windows machine, then it can monitor any type of host but if the server is running in Linux, then it can monitor Windows, only if an SNMP agent is running in it. Also, any type of user can be used to log into Linux, whereas Admin users only can log into Windows.

**See Also**

Monitor Information - Server | Create Other New Monitors
HTTP URL Monitors

In an environment, where downtime of any website applications and services can cause negative impact on the business performance, problems must be accurately identified and solved. Applications Manager acts as a continuous URL monitoring service that keeps a constant watch over the specified URL or website pages. They test the website applications and web services to ensure that they are functioning properly.

URL monitors verify the availability of specified, addressable, standard HTTP and HTTPS URLs. They scan the HTTP and HTTPS pages looking for a predefined keyword to check whether the website is available.

There are two ways of URL monitoring provided by Applications Manager.

- **HTTP-URLs**
- **HTTP-URL Sequence**

The difference between the two types of monitoring is that URL Monitoring monitors single HTTP and HTTPS URL, whereas URL sequence monitors a set of HTTP and HTTPS URLs in sequence. Also, any HTTP and HTTPS URL can be monitored using URL Monitoring, provided they require no authentication details.

Please go through the following sections to know about the configuration details.

**HTTP-URLs**

To configure for URL monitoring, follow the given steps:

1. Select **New Monitor**. From the combo box, choose **HTTP-URLs**.
2. Provide any **display name** for the HTTP-URL monitoring.
3. Provide the HTTP/HTTPS **URL address**, you want to monitor.
4. Enter any keyword as **match content**. The URL monitoring searches the keyword in the content of the URL page to check the availability of the URL. This is optional.

   **Note**: The content search is case-sensitive. If you provide 2 words, the content match is performed for the words separately. For example, if you specify the content as **applications manager**, the match is found for **applications** and **manager** separately. If you need the content match to be performed for the complete text, specify the 2 words in quotes, example "**applications manager**".

5. Provide the **polling interval** for which Applications Manager updates the status of the monitor.
6. Choose between the **Post and Get**, which are the two types of Form method for any HTTP/HTTPS URL.
7. Click **Add URL Monitor** to initiate monitoring of the specified URL.

Apart from the basic URL Monitoring, Applications Manager also provides you with advanced options that furnish effective and more flexible URL Monitoring. This is optional and you need to choose these options only if the HTTP/ HTTPS URL requires **Form-based authentication**.

1. Provide the request parameters, if any. The request parameters must be provided as name=value pairs for Post and Get methods. For example, if you want to monitor a URL like, http://appmanager:9090/showresource.do?haid=1&type=UrlMonitor&method=getMonitorForm, then provide "?haid=1&type=UrlMonitor&method=getMonitorForm" as request parameter.
2. Enter a keyword which when matches with the content in the URL must be notified of error in Error If Match field. Note: The search is case sensitive.

3. Enter the Response Code details by choosing them from the combo box. By default, it is greater than 200. Hence the error will be notified once the criteria mentioned are met.

4. Enter the time, in minutes, for which the URL monitor should wait for a page to complete downloading before timing out in Time out field.

5. Check "If monitor detects error, re-try immediately to verify error", where the monitoring is automatically performed when it detects an error, i.e. when an error is detected, the monitor will immediately be scheduled to run again once.

6. Provide the User name and password, if the URL requires Form-based authentication.

Note: To monitor NTLM authenticated URLs, copy the cryptix-jce-provider.jar from http://www.cryptix.org/cryptix-jce-20050328-snap.zip and extract to <AppMgr Home>/lib/ext.

HTTP-URL Sequence

The purpose of URL Sequence is to monitor multiple web pages of an online application. It checks pages with dynamically generated information enhancing interactive transactions such as logging into a login page, creating an account using a web form, instructing the application to perform some action, etc.

URL Sequencing starts with a specific URL such as the Login page and then followed by additional links/URL in it. The URL Sequence monitoring thus performs end-to-end verification of particular transactions helping you to troubleshoot any problems while monitoring.

Note: If you are connecting to an URL using a proxy server, then you must configure proxy to initiate the URL sequence monitoring. Refer to the Configuring Proxy section of Performing Admin Activities, for further details.

There are two methods to configure a URL Sequence,

1. URL Sequence Recorder:

You can use the recorder.exe that is bundled with Applications Manager to automatically configure the URL Sequence. Recorder.exe is found under the /bin directory.

On running the exe, the URL Sequence Recorder console and Control Panel is opened up. Follow the steps given below to configure the URL Sequence:

- Enter the URL address that you want to monitor and click on 'Go'.
- Via the UI, Click on the sequences that you want to monitor.
- Click on Save Sequence, once you are finished with the sequence. This will save the URL Sequence in Applications Manager.
- Enter the URL SequenceName.
- Enter the Polling Interval. The default is 5 minutes.
- Enter the Host and Port number of Applications Manager.
- Enter the user and password of Applications Manager.
- You can view the newly created URL Sequence in the Applications Manager Web Client.
Control Panel:

You can edit the URL Sequence with the help of Control Panel. The Control Panel lists down all the recorded URLs in the particular Sequence. Deletion of recorded URLs is possible using the del key.

Label:

Select any URL and enter the URL Label with which the URL would be identified, under URL Details.

Alert Mechanism:

Alerts would be generated if you select the three options given

- if the following keywords are found: Enter the keywords associated with the URL, the presence of those would trigger an alert. For e.g., ErrorCode
- if the following keywords are not found: Enter the keywords associated with the URL, the absence of those would trigger an alert
- if response code is: Select the response code for which alert should be generated.

Basic Authentication:

If the URLs require basic authentication, then enter the Username and Password.

2. Creating a new HTTP-URL Sequence monitor through Applications Manager webclient:

1. Select New Monitor. From the combo box, choose HTTP-URL Sequence.
2. Provide any Display Name for the URL sequence monitoring.
3. Enter the URL Address of a web page such as the Login page of a website.
4. Enter any html content that is used to check the availability of the URL. This is optional.
   
   Note: The content search is case-sensitive. If you provide 2 words, the content match is performed for the words separately. For example, if you specify the content as applications manager, the match is found for applications and manager separately. If you need the content match to be performed for the complete text, specify the 2 words in quotes, example "applications manager".
5. Provide the polling interval time for which Applications Manager updates the status of the monitor.
6. Provide the Form Submission Method. You can provide Post or Get request parameters for the URL.
7. Click Add URL to start monitoring the specified URL. This opens a screen listing the previous URL address and you can configure for the next URL. The details are given below:

   1. Choose any of the 4 options of Links, Forms, Frames, and Other URLs. The details are given below:

      - Link: This lists all the available links/URLs in the starting or Login page URL in a combo box.
      - Form: This lists all the names of Form type available in the Login page URL in a combo box. The required parameters of the form will be listed for input values in a text box provided below the combo box. Fill the parameters with value.
      - Frame: This lists all the frames of the URL being monitored, in a combo box. Select the URL of the frame.
      - Other: You can enter the URL you want to request along with any name-value pairs needed to get to the next sequence step, even if those values are available through some other page element (such as a form).
2. Click either **Add URL**, if you want to continue the sequence. Click **Add URL and Finish** to add the URL and finish the sequence. Click **Finish** to complete the URL Sequence monitoring without adding the current sequence. The URL Sequence is a repetitive process depending on the number of web pages and actions, and you have to follow the above step 1 and step 2 to complete the sequence.

URL Sequence Monitoring also has advanced options that need to be followed for URLs with Form-based authentication. Refer to the steps (2-6) of **URL Monitoring Advanced Options** to know details on advanced options.

**See Also**

Monitor Information - HTTP URL Monitors | Create Other New Monitors
Custom Monitors

Custom Monitors provide a way to monitor

1. Java applications or other applications that expose management information through SNMP (Simple Network Management Protocol) and JMX (Java Management Extensions) - **JMX / SNMP DashBoard**
2. the output of in-house custom scripts (Windows/Linux) - **Script Monitors**
3. AdventNet QEngine Webperformance script, AdventNet QEngine is an automated testing platform for testing of Back-End & Middle-tier (server-side) and Web (Record & Play) functionality and performance of J2EE/J2SE applications - **QEngine Script Monitors**

**JMX / SNMP Dash Board**

For example, you have a Java application with built-in manageability using JMX and any application that has an SNMP interface, then they are managed by building JMX/SNMP DashBoard.

To create a JMX / SNMP Dash Board, follow the given steps:

1. Select **New Monitor**. From the combo box, choose **JMX / SNMP DashBoard**.
2. Provide any **name** for the custom monitor and a **description**.
3. Click **Add JMX / SNMP DashBoard** to create the custom monitor. This opens a screen that allows you to add attributes for custom monitors.

The next step is to build the custom monitor to enable monitoring your data sources. Refer to the **Custom Monitors** section of Monitor Information, for more details on the same.

**Note**: To monitor **Custom WebSphere attributes**, the following changes need to be done for Applications Manager to monitor them.

```
1. Copy the following jars from <WebSphere installed directory>/lib/ to <Applications Manager Home>/lib/was directory.
   o  admin.jar
   o  bootstrap.jar
   o  ffdc.jar
   o  idl.jar
   o  iwsorb.jar
   o  j2ee.jar
   o  jfltl.jar
   o  jmxc.jar
   o  jmxr.jar
   o  pmi.jar
   o  pmiclient.jar
   o  ras.jar
   o  sas.jar
   o  soap.jar
   o  utilis.jar
   o  wasjmx.jar
   o  wsexception.jar
   o  wssec.jar
```
2. Copy the following jars from `<WebSphere Installed Directory>/java/jre/lib/ext` to `<Applications Manager Home>/lib/was` directory.
   - log.jar
   - mail.jar

3. **For Windows and Linux Installation of WebSphere:** Copy the `security.jar` from `<WebSphere installed directory>/java/jre/lib/` to `<Applications Manager Home>/lib/was` directory.

   **For Solaris Installation of WebSphere:** Copy the `ibmjsse.jar` from `<WebSphere Installed Directory>/java/jre/lib/` to `<Applications Manager Home>/lib/was` directory and rename it as `security.jar`.

You need to discover JMX MBeans and SNMP Agent data source to add attributes. The following are the JMX MBean resources whose MBean attributes are monitored by Applications Manager using Custom Monitor:

- AdventNet JMX Agent- RMI Adapter
- JMX [MX4J / JDK 1.5]
- WebLogic Server
- JBoss Server
- WebSphere Server

💡 **Troubleshoot:** Having trouble in monitoring custom applications? Refer to the online Troubleshooting section.

**See Also**

- Monitors - Custom Monitor | Create Other New Monitors
Script Monitors

Custom script monitoring can be a tedious task if the output of the scripts that are run, are to be monitored manually. Applications Manager provides with script monitoring functionality to ease the process by automatically monitoring the output of in-house custom scripts (Windows/Linux) and by creating alerts as per the configuration.

To add Script Monitor, follow the given steps:

1. Click **New Monitor.** From the combo box, choose **Script Monitor.**
2. Enter the **Display Name** of the Monitor.
3. Give the absolute path of the **Script to be Monitor** and also the absolute path of the directory from which the script should be executed.
4. Give the **Output file name** with absolute path.
5. Enter the Name of the **String** and **Numeric** attributes.
6. Enter the value of **Delimiter** used in the output file. By default, it is ":". If you don't specify a delimiter, then 'space' would be considered as a delimiter.
7. Specify the **Arguments**. For e.g., hostname 80 http
8. Enter the **Polling Interval.** By default, it is 5 minutes
9. Specify the **Timeout** value in seconds. The value can be the maximum time taken by the script to execute.
10. In Linux, Specify the **mode** in which script should be executed. By default, it is "sh".
11. Upon adding the script monitor, you can view the details of the newly added Script Monitor

See Also

Monitor Information - Script Monitors | Create Other New Monitors
QEngine Script Monitors

Applications Manager provides with AdventNet QEngine script monitoring functionality to automatically monitor the QEngine Webperformance script. AdventNet QEngine is an automated testing platform for testing of Back-End & Middle-tier (server-side) and Web (Record & Play) functionality and performance of J2EE/J2SE applications. More information on QEngine is available here.

To add QEngine Script Monitor, follow the given steps:

1. Click New Monitor. From the combo box, choose QEngine Script Monitor.
2. Enter the Display Name of the Monitor.
3. Give the absolute path of the testcase file (.tst) as QEngine Script File Path.
4. Enter the Polling Interval. By default, it is 5 minutes
5. Specify the Timeout value in seconds. The value can be the maximum time taken by the script to execute. By default it is 60 seconds. If the script execution is not completed within the specified timeout period Applications Manager reports the webperformace test as failed.
6. In Linux, Specify the mode in which script should be executed. By default, it is “sh”.
7. Upon adding the QEngine script monitor, you can view the details of the newly added QEngine Script Monitor

See Also

Monitor Information - QEngine Script Monitors | Create Other New Monitors
Web Transaction Monitor

Using Web Transaction Monitor, you can monitor End-to-End Web Transactions starting from the URL to SQL. Further, you would be able to have a drill down view of the WEB components, EJB, Java and SQL statements of the URL. Individual methods of the various J2EE and Java components can be monitored to identify performance bottlenecks.

PreRequisite: Web Transaction Monitor requires an agent to be plugged in the application server (like JBoss) to be monitored. Know more about the agent.

Follow the steps given below to create a Web Transaction monitor:

- Click New Monitor. From the combo box, choose Web Transaction.
- Enter the Host Name or the IP Address of the Host whose web transactions you want to monitor.
- Enter the SubNetMask of the network.
- Provide the port number in which the web transaction agent is running.
- Enter the polling interval time in minutes. Default is 5 minutes.
- Choose the Monitor Group, to which you want to associate the Monitor (optional).
- Click Add Monitor(s). This discovers the Monitor from the network and starts monitoring them.

Note: The Web Transaction Monitor supports JDK1.5 only.

See Also

Monitor Information - Web Transactions Monitor | Create Other New Monitors
Monitor Information

Applications Manager is used to monitor different types of applications and services of Monitor running in your system/ network. Monitoring is an activity that checks the performance of your monitors by collecting and analyzing the data at regular intervals. These monitoring capabilities are performed by different types of Monitor Types.

This chapter lists the different types of Monitor Types supported by Applications Manager and the parameters monitored by them.

Types of Monitor Types

Applications Manager supports the following Monitor Types:

1. Application Servers
   - Microsoft .NET
   - JBoss Servers
   - Oracle Application Servers
   - Tomcat Servers
   - WebLogic Servers
   - WebSphere Servers

2. Transaction Monitors
   1. Web Transactions

3. Database Servers
   - MySQL Database Servers
   - Oracle Database Servers
   - MS SQL Database Servers
   - IBM DB2 Database Server

4. Servers
   - Windows
   - Linux
   - Solaris
   - IBM AIX
   - HP Unix
   - Tru64 Unix
   - Free BSD

5. Mail Servers
   - Exchange Server
   - Mail Server

6. Web Services
   - Apache Server
   - IIS Server
   - PHP
   - Web Server
   - HTTP URL Monitors and HTTP URL Sequence
7. Services
   o JMX [MX4J / JDK 1.5]
   o Service Monitoring
   o AdventNet JMX Agent - RMI Adapter
   o SNMP
   o Telnet

8. Custom Monitors
   1. JMX / SNMP Dashboard.
   2. Script Monitor
   3. QEngine Script Monitor
Application Servers

Application Servers are designed to develop web services and applications, and in real time, the productivity and performance of such servers get affected due to failure of diagnosing any problem in the services/application running in the server.

Applications Manager enables high performance business process management by detecting and diagnosing problems of application servers and their services faster. The following are the application servers supported:

- Microsoft .NET
- JBoss Servers
- Oracle Application Servers
- Tomcat Servers
- WebLogic Servers
- WebSphere Servers

Please browse through the different application servers that provide the server information and their parameters being monitoring.

See Also

Creating New Monitor - Application Server
Microsoft .NET

Monitored Parameters

Microsoft .NET is monitored based on the attributes such as Heap Size, Threads etc. The monitoring details of Microsoft .Net are represented graphically and that helps to understand the parameters with ease. You can also configure thresholds to the attributes monitored by the .Net, based on these details.

The following table lists down the parameters that are monitored for Microsoft .NET. Click on the Microsoft .NET Monitor listed in your Monitor Group to view these information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Shows the current status of the .Net - available or not available.</td>
</tr>
<tr>
<td>Threads</td>
<td></td>
</tr>
<tr>
<td>Physical Threads</td>
<td>Shows the number of native OS threads created &amp; owned by the CLR to act as underlying threads for .NET thread objects.</td>
</tr>
<tr>
<td>Logical Threads</td>
<td>Shows the number of current .NET thread objects in the application.</td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>Heap Size</td>
<td>Shows the current memory allocated(MB)</td>
</tr>
<tr>
<td>% Time in GC</td>
<td>Shows the percentage of elapsed time that was spent in performing a garbage collection (GC) since the last GC cycle. This counter is usually an indicator of the work done by the Garbage Collector on behalf of the application to collect and compact memory.</td>
</tr>
<tr>
<td>Locks</td>
<td></td>
</tr>
<tr>
<td>Queue Length</td>
<td>Refers to the total number of threads currently waiting.</td>
</tr>
<tr>
<td>Contentions/Min</td>
<td>Refers to the rate at which threads in the runtime attempt to acquire a managed lock unsuccessfully.</td>
</tr>
<tr>
<td>Exceptions</td>
<td></td>
</tr>
<tr>
<td>Exceptions/Min</td>
<td>Refers to the number of exceptions per Minute</td>
</tr>
<tr>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td>Connections/Min</td>
<td>Refers to the number of connections per Minute</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>TotalRuntimeChecks/Min</td>
<td>Refers the total number of runtime Code Access Security (CAS) checks performed per minute.</td>
</tr>
<tr>
<td>JIT</td>
<td></td>
</tr>
<tr>
<td>% Time In JIT</td>
<td>Refers to the percentage of elapsed time spent in JIT compilation since the last JIT compilation phase.</td>
</tr>
<tr>
<td>Network Traffic</td>
<td></td>
</tr>
<tr>
<td>Bytes Sent/Min</td>
<td>Refers to the number of Bytes sent per minute</td>
</tr>
<tr>
<td>Bytes received/Min</td>
<td>Refers to the number of Bytes received per minute</td>
</tr>
</tbody>
</table>
The various .NET application's parameters that are monitored are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Request Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Requests/Min</td>
<td>Refers to number of Requests executed per minute</td>
</tr>
<tr>
<td>Errors/Min</td>
<td>Refers to rate of errors occurred</td>
</tr>
<tr>
<td>Requests</td>
<td>Refers to number of Requests Timeout per minute</td>
</tr>
<tr>
<td>Timeout/Min</td>
<td>Refers to number of Queued Requests</td>
</tr>
<tr>
<td>Queued Requests</td>
<td></td>
</tr>
<tr>
<td><strong>Transactions</strong></td>
<td></td>
</tr>
<tr>
<td>Transactions/Min</td>
<td>Refers to number of Transactions started per minute</td>
</tr>
<tr>
<td>Abandoned</td>
<td>Refers to number of Transactions aborted per minute</td>
</tr>
<tr>
<td>Pending Transactions</td>
<td>Refers to number of Transactions in progress</td>
</tr>
<tr>
<td><strong>Sessions</strong></td>
<td></td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Refers to number of sessions that are active currently</td>
</tr>
<tr>
<td><strong>Network Traffic</strong></td>
<td></td>
</tr>
<tr>
<td>Bytes Sent/Min</td>
<td>Refers to the number of Bytes sent per minute</td>
</tr>
<tr>
<td>Bytes Received/Min</td>
<td>Refers to the number of Bytes received per minute</td>
</tr>
</tbody>
</table>

**See Also**

*Creating New Monitor - Microsoft .NET*
JBoss Servers

Supported Versions

Applications Manager supports monitoring of JBoss Servers of versions 3.2.x, 4.0.1, 4.0.2, 4.0.3. For help in monitoring other versions of JBoss 4.X, contact support@appmanager.com

Monitored Parameters

JBoss servers are monitored based on the attributes such as JVM heap Usage, Response time, etc. and the different web applications and EJB deployed in the server. The monitoring details of JBoss server are represented graphically that helps to understand the parameters with ease. You can also configure thresholds to the attributes monitored by the server based on these details.

The following table lists down the parameters that are monitored for JBoss Servers. Click on the JBoss server Monitor listed in your Monitor Group to view these information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Information</td>
<td></td>
</tr>
<tr>
<td>JBoss Version</td>
<td>The version of the JBoss Server.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The port at which the JBoss server listens.</td>
</tr>
<tr>
<td>Web Server Port</td>
<td>The port at which web server service is running.</td>
</tr>
<tr>
<td>Activation Time</td>
<td>Specifies the time when the JBoss Server was started.</td>
</tr>
<tr>
<td>Monitoring Started Time</td>
<td>Specifies the time when the monitoring of the server was started.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
<tr>
<td>JVM Usage</td>
<td>Refers to the current amount of free and used memory in the JVM heap in kilobytes.</td>
</tr>
<tr>
<td>Server Response Time</td>
<td>Refers to the time required for the server to respond while monitoring.</td>
</tr>
<tr>
<td>Web Applications Details</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Web Application</td>
</tr>
<tr>
<td>Context Root</td>
<td>Specifies a context root of the Web application.</td>
</tr>
<tr>
<td>Response Type</td>
<td>Lists the different HTTP status code that are obtained for every request sent to web applications.</td>
</tr>
<tr>
<td>Total Number of Requests</td>
<td>The number of requests for each response types.</td>
</tr>
<tr>
<td>Average requests per Data Collection Cycle</td>
<td>The average requests processed for every data collection cycle.</td>
</tr>
<tr>
<td>Servlet Details</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the servlet.</td>
</tr>
<tr>
<td>Execution Time</td>
<td>Specifies the total execution time, in milliseconds, for the servlet.</td>
</tr>
<tr>
<td>Invocation Count</td>
<td>Specifies the number of times that the servlet is invoked, i.e. the hits of the Servlet.</td>
</tr>
<tr>
<td>Enterprise Java Bean Details</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the EJB</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the EJB - Entity Bean, Stateless Session Bean, Stateful Session Bean, and Message Driven Bean.</td>
</tr>
<tr>
<td>Module</td>
<td>Refers to the jar to which the EJB belongs.</td>
</tr>
<tr>
<td>Number of Instances Created</td>
<td>Specifies the total number of EJB instances created.</td>
</tr>
<tr>
<td>Number of Instance Removed</td>
<td>Specifies the total number of EJB instances destroyed.</td>
</tr>
<tr>
<td>Number of Instances</td>
<td>Specifies the total number of EJB instances that are available for</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Available for Processing</td>
<td>processing requests.</td>
</tr>
<tr>
<td>Number of Instances in ready state</td>
<td>Specifies the total number of EJB instances that are in ready state.</td>
</tr>
<tr>
<td>Number of Instances in Pooled state</td>
<td>Specifies the total number of EJB instances that are in pooled state.</td>
</tr>
<tr>
<td><strong>JDBC Connection Pool Details</strong></td>
<td></td>
</tr>
<tr>
<td>JDBC Pool</td>
<td>Name of the Connection Pool.</td>
</tr>
<tr>
<td>Pool Size</td>
<td>Number of connections in the pool.</td>
</tr>
<tr>
<td>Connections Currently in Use</td>
<td>Number of connections that are currently being used.</td>
</tr>
<tr>
<td>Connections created</td>
<td>Total number of connections that have been created after the pool was instantiated.</td>
</tr>
<tr>
<td>Connections destroyed</td>
<td>Total number of connections that have been destroyed after the pool was instantiated.</td>
</tr>
<tr>
<td>Idle Time Out (Mins)</td>
<td>Maximum number of minutes that an idle (unallocated) connection can remain in the pool before being removed to free resources.</td>
</tr>
</tbody>
</table>

**Custom Attributes**
You can also view the custom attributes of the JBoss Server in the same page. Click **Add Attributes** to add custom JBoss attributes. For information on adding Custom Monitors, refer to **Custom Monitors topic**.

**See Also**

Creating New Monitor - JBoss Server
Oracle Application Servers

Supported Versions

Applications Manager supports monitoring of Oracle Application Servers 10g.

Monitored Parameters

Oracle Application servers are monitored based on the attributes listed below. The monitoring details of Oracle Application server are represented graphically that helps to understand the parameters with ease. You can also configure thresholds to the attributes monitored by the server based on these details.

The following table lists down the parameters that are monitored for Oracle Application Servers. Click on the Oracle Application server Monitor listed in your Monitor Group to view these information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitor Information</strong></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>The port at which the Oracle Application server listens.</td>
</tr>
<tr>
<td>Last Polled at</td>
<td>Specifies the time when the monitoring of the server was started.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
<tr>
<td><strong>Request Throughput</strong></td>
<td>Number of requests processed per unit of time in the server.</td>
</tr>
<tr>
<td>Throughput</td>
<td></td>
</tr>
<tr>
<td>Current Active Connection</td>
<td>Shows the current active connections</td>
</tr>
<tr>
<td>Average Connection Process Time</td>
<td>Gives the average processing time of the connections</td>
</tr>
<tr>
<td>Current Active Request</td>
<td>Shows the number of requests that are active currently</td>
</tr>
<tr>
<td><strong>Server Response Time</strong></td>
<td>Refers to the time required for the server to respond while monitoring.</td>
</tr>
<tr>
<td>Response Time</td>
<td></td>
</tr>
<tr>
<td>Data Throughput</td>
<td>Refers to how much data is transferred per unit time</td>
</tr>
<tr>
<td>Data Processed</td>
<td>Refers to how much data is processed per request</td>
</tr>
<tr>
<td>Servlets</td>
<td>Total number of servlets</td>
</tr>
<tr>
<td><strong>OPMN Process Memory Stats</strong></td>
<td>Memory statistics of the OPMN processes like dcm-daemon, WebCache, WebCache Admin, HTTP_Server, home</td>
</tr>
<tr>
<td>Used Memory</td>
<td>Gives the total physical memory used by the process</td>
</tr>
<tr>
<td><strong>oc4j JVM Statistics</strong></td>
<td>Shows the number of Active Thread groups in the JVM</td>
</tr>
<tr>
<td>Active Thread Groups</td>
<td>Shows the number of Active Threads in the JVM</td>
</tr>
<tr>
<td>Active Threads</td>
<td>Shows current heap memory usage of the process</td>
</tr>
<tr>
<td>Heap Usage</td>
<td>Gives the total number of JDBC Connections</td>
</tr>
<tr>
<td>JDBC Connections</td>
<td>Gives the total number of open, committed and aborted JDBC transactions</td>
</tr>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td><strong>Web Applications</strong></td>
<td>Total number of servlets in the web application</td>
</tr>
<tr>
<td>Servlets</td>
<td>Number of requests processed per unit of time in the web application</td>
</tr>
<tr>
<td>Throughput</td>
<td>Time taken to process the request</td>
</tr>
<tr>
<td>Process Request</td>
<td>Current number of active requests for the web application</td>
</tr>
<tr>
<td>Active Request</td>
<td>Number of active sessions of the web application</td>
</tr>
<tr>
<td>Active Session</td>
<td>Total time for which the sessions have been active</td>
</tr>
<tr>
<td>Session time</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>JMS Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>Deque Avg</td>
<td>Average time to deque messages</td>
</tr>
<tr>
<td>Enque Avg</td>
<td>Average time to enque messages</td>
</tr>
<tr>
<td>Pending Message</td>
<td>Total number of message waiting to be processed</td>
</tr>
<tr>
<td>Message Dequeued</td>
<td>Total number of messages dequeued</td>
</tr>
<tr>
<td>Message Enqueued</td>
<td>Total number of messages enqueued</td>
</tr>
<tr>
<td>Message Count</td>
<td>Number of messages in the JMS Destination</td>
</tr>
<tr>
<td><strong>EJB Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>EAR Name</td>
<td>Name of the Enterprise Application Resource</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the oc4j process to which the EJB belongs to</td>
</tr>
<tr>
<td>Type</td>
<td>Gives the type of the EJB</td>
</tr>
<tr>
<td>Create Count</td>
<td>Number of EJBs created</td>
</tr>
<tr>
<td>Active Count</td>
<td>Number of active EJBs</td>
</tr>
<tr>
<td>Passive Count</td>
<td>Number of passive EJBs</td>
</tr>
<tr>
<td>Pooled Count</td>
<td>Number of pooled EJBs</td>
</tr>
<tr>
<td><strong>Response Summary</strong></td>
<td>Gives the count for the various HTTP responses</td>
</tr>
</tbody>
</table>

**See Also**

[Creating New Monitor - Oracle Application Server](#)
Tomcat Servers

Supported Versions

Applications Manager supports monitoring of the following versions of the Tomcat Servers:

1. Tomcat 3.x
2. Tomcat 4.x
3. Tomcat 5.x

Monitored Parameters

Tomcat Servers are monitored based on the parameters or the attributes listed below. These attributes provide information about the functioning of the Monitors of Tomcat server. You can also configure thresholds to the numerical attributes monitored by the server based on these details.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
<tr>
<td>Average Response Time</td>
<td>Refers to the average time, in milliseconds, for getting a response.</td>
</tr>
<tr>
<td>Requests per Second</td>
<td>Specifies the number of requests received by the server in one second.</td>
</tr>
<tr>
<td>Average Bytes per Second</td>
<td>Refers to the average bytes per second.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>Specifies the total memory of the server in mega bytes.</td>
</tr>
<tr>
<td>Used Memory</td>
<td>Specifies the used memory of the server in mega bytes.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Specifies the free memory of the server in mega bytes.</td>
</tr>
<tr>
<td>Busy Threads</td>
<td>Specifies the number of threads busy i.e that are currently used.</td>
</tr>
<tr>
<td>Current Threads</td>
<td>Specifies the number of created threads that are available for use.</td>
</tr>
<tr>
<td>Response Summary</td>
<td>Contains Response Type that specifies the count of the response in each type.</td>
</tr>
<tr>
<td>Application Summary</td>
<td>Lists different web applications such as servlets, running in the server.</td>
</tr>
<tr>
<td></td>
<td>Click on the application names to view details.</td>
</tr>
</tbody>
</table>

The data displayed differs between each version of the Tomcat Server.

Data displayed for Tomcat 3.x

1. Availability
2. Memory Usage

Data displayed for Tomcat 4.x

1. Availability
2. Response Time Details
3. Memory Usage
4. Response Summary
5. Application Summary and Details
6. Memory Usage
7. Response Summary
Data displayed for Tomcat 5.x

1. Availability
2. Response Time Details
3. Memory Usage
4. Thread Details
5. Response Summary
6. Application Summary and Details.

See Also

Creating New Monitor - Tomcat Server
WebLogic Servers

Supported Versions

The following versions of the WebLogic Servers can be monitored by the Applications Manager:

1. WebLogic 6.1
2. WebLogic 7.x
3. WebLogic 8.x
4. WebLogic 9.0
5. WebLogic 9.1

Monitored Parameters

WebLogic servers are monitored based on a few parameters or the attributes. These attributes provide information about the functioning of the Monitors of WebLogic server and you can also receive alerts based on the thresholds configured on the numerical attributes of the server.

The table below lists the WebLogic Server parameters that are monitored.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitor Details</strong></td>
<td></td>
</tr>
<tr>
<td>WebLogic Version</td>
<td>Refers to the version of the WebLogic Server.</td>
</tr>
<tr>
<td>State</td>
<td>Refers to the server state such as running and down.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>Specifies the port at which the WebLogic Server listens for connections.</td>
</tr>
<tr>
<td>Activation Time</td>
<td>Specifies the time when the WebLogic Server was started.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
<tr>
<td>JVM Heap Size</td>
<td>Refers to the current size of the JVM heap in kilobytes.</td>
</tr>
<tr>
<td>Server Response Time</td>
<td>Refers to the time required for the server to respond while monitoring.</td>
</tr>
<tr>
<td><strong>Web Application Details</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Web Application.</td>
</tr>
<tr>
<td>Number of Active Sessions</td>
<td>Specifies the number of sessions that are currently active in the Application.</td>
</tr>
<tr>
<td>Maximum Number of Sessions</td>
<td>Refers to the highest number of sessions that were open for an Application.</td>
</tr>
<tr>
<td>Total Number of Sessions</td>
<td>Refers to the total number of sessions that were opened since deployment of an Application.</td>
</tr>
<tr>
<td>Number of Servlets</td>
<td>Refers to the total number of servlets of a web application. Click on the number, to find details on Servlets as explained below.</td>
</tr>
<tr>
<td><strong>Servlet Details</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the servlet.</td>
</tr>
<tr>
<td>Execution Time</td>
<td>Specifies the total execution time, in milliseconds, for the servlet.</td>
</tr>
<tr>
<td>Invocation Count</td>
<td>Specifies the number of times that the servlet is invoked, i.e. the hits of the Servlet.</td>
</tr>
<tr>
<td><strong>Enterprise Java Bean Details</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the JNDI name of the Bean with JAR and EAR name. Move the mouse pointer over the EJB name to view the JAR and EAR name.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the bean type - Entity, Stateless Session, Stateful Session, and Message Driven beans</td>
</tr>
<tr>
<td>Activation Count</td>
<td>Refers to the total number of beans activated (i.e. from the Secondary storage to Primary storage) for that particular Bean container.</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passivation Count</td>
<td>Refers to the total number of beans passivated (i.e. from the Primary storage to Secondary storage) for that particular Bean container.</td>
</tr>
<tr>
<td>Threads Waiting</td>
<td>Specifies the total count of idle threads assigned in the thread queue.</td>
</tr>
<tr>
<td>Cached Beans Current Count</td>
<td>Refers to the number of Cached Beans in the container.</td>
</tr>
<tr>
<td>Beans In Use Count</td>
<td>Specifies the number of beans currently in use.</td>
</tr>
<tr>
<td>Idle Beans Count</td>
<td>Specifies the number of beans that are currently idle.</td>
</tr>
<tr>
<td>Transaction Timed Out Count</td>
<td>Specifies the total number of transactions, which have been rolled back due to timeout.</td>
</tr>
<tr>
<td>Transaction Rolled Back Count</td>
<td>Refers to the total number of transactions that are rolled back.</td>
</tr>
<tr>
<td>Transaction Committed Count</td>
<td>Refers to the number of transactions committed or completed successfully.</td>
</tr>
</tbody>
</table>

### Database Connection Pools Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the database connection pools that enables caching of database connection in the monitor easier through pools.</td>
</tr>
<tr>
<td>Connection Pool Size</td>
<td>Specifies the number of database connection pool.</td>
</tr>
<tr>
<td>Active Connections</td>
<td>Mentions the number of active connections made to the monitor.</td>
</tr>
<tr>
<td>Leaked Connections</td>
<td>There can be some problems in connections that are checked out from the connection pool but are not returned back to the pool and they are specified using the parameter.</td>
</tr>
<tr>
<td>Thread Waiting</td>
<td>Mentions the number of threads waiting for the connection.</td>
</tr>
</tbody>
</table>

### Thread Pools Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the thread pools.</td>
</tr>
<tr>
<td>Total Threads</td>
<td>Refers to the total count of threads assigned in this thread queue.</td>
</tr>
<tr>
<td>Idle Threads</td>
<td>Specifies the threads that are idle or not used.</td>
</tr>
<tr>
<td>Threads In Use</td>
<td>Specifies the threads that are currently in use.</td>
</tr>
<tr>
<td>Pending Requests Count</td>
<td>Specifies the number of requests that are pending in the queue.</td>
</tr>
</tbody>
</table>

### Custom Attributes

You can also view the custom attributes of the WebLogic Server in the same page. Click **Add Attributes** to add custom WebLogic attributes. For information on adding Custom Monitors, refer to [Custom Monitors topic](#).

### See Also

[Creating New Monitor - WebLogic Server](#)
WebSphere Servers

Supported Versions

The following version of the WebSphere Servers can be monitored by the Applications Manager:

- WebSphere Version 5.x, 6.x

Monitored Parameters

WebSphere servers are monitored based on the following parameters or the attributes listed in the table. The monitoring details of the server are represented graphically that helps to understand the parameters with ease. You can also configure thresholds to the attributes monitored by the server based on these details.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Details</td>
<td>Denotes the version of the WebSphere server monitor.</td>
</tr>
<tr>
<td>WebSphere Version</td>
<td>Denotes the version of the WebSphere server monitor.</td>
</tr>
<tr>
<td>State</td>
<td>Refers to different states of the Websphere server such as running and down.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>Refers to HTTP Transport port.</td>
</tr>
<tr>
<td>Transaction Details</td>
<td>Specifies Global Commit Duration, Committed Transactions, Transactions Rolled Back and Transactions Optimized.</td>
</tr>
<tr>
<td>Availability</td>
<td>Specifies the status of the WebSphere server - available or not available.</td>
</tr>
<tr>
<td>JVM Memory Usage</td>
<td>Specifies the total memory in JVM run time.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Specifies the average system CPU utilization taken over the time interval since the last reading.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Specifies the amount of real free memory available on the system.</td>
</tr>
<tr>
<td>Average CPU Utilization</td>
<td>Specifies the average percent CPU Usage that is busy after the server is started.</td>
</tr>
<tr>
<td>Session Details of Web Applications</td>
<td>The total number of requests received for sessions that were last accessed from other Web applications. This value can indicate failover processing or a corrupt plug-in configuration.</td>
</tr>
<tr>
<td>User Sessions</td>
<td>Specifies the total number of sessions that were created.</td>
</tr>
<tr>
<td>Invalidated Sessions</td>
<td>Specifies the total number of sessions that were invalidated.</td>
</tr>
<tr>
<td>Affinity Breaks</td>
<td>Mentions the names of the different EJB present in the WebSphere server with JAR and EAR name. Move the mouse pointer over the EJB name to view the JAR and EAR name.</td>
</tr>
<tr>
<td>Type</td>
<td>Denotes the different types of the bean such as entity, stateless session, stateful session, and message driven.</td>
</tr>
<tr>
<td>Concurrent Lives</td>
<td>Specifies the number of concurrent live beans.</td>
</tr>
<tr>
<td>Total Method Calls</td>
<td>Specifies the total number of method calls.</td>
</tr>
<tr>
<td>Average Method Response Time</td>
<td>Specifies the average time required to respond to the method calls.</td>
</tr>
<tr>
<td>Pool Size</td>
<td>Specifies the number of objects in the pool (entity and stateless).</td>
</tr>
<tr>
<td>Activation Time</td>
<td>Specifies the average time in milliseconds that the total bean is activated</td>
</tr>
</tbody>
</table>
### Parameters
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>for that particular Bean container, including the time at the database, if any.</td>
</tr>
</tbody>
</table>

### Current JDBC Connection Pool Details
- **Name**: Mentions the name of the current JDBC Connection pool.
- **Pool Type**: Refers to the type of the connection pool.
- **Create Count**: Refers to the total number of connections created.
- **Pool Size**: Specifies the size of the connection pool.
- **Concurrent Waiters**: Specifies the number of threads that are currently waiting for a connection.
- **Faults**: Specifies the total number of faults in the connection pool such as timeouts.
- **Average Wait Time**: Specifies the average waiting time, in milliseconds, until a connection is granted.
- **Percent Maxed**: Specifies the average percent of the time that all connections are in use.

### Thread Pool Details
- **Name**: Mentions the name of the thread pool.
- **Thread Creates**: Specifies the total number of threads created.
- **Thread Destroys**: Specifies the total number of threads destroyed.
- **Active Threads**: Specifies the number of concurrently active threads.
- **Pool Size**: Specifies the average number of threads in pool.
- **Percent Maxed**: Specifies the average percent of the time that all threads are in use.

### Custom Attributes
You can also view the custom attributes of the WebSphere Server in the same page. Click **Add Attributes** to add custom WebSphere attributes. For information on adding Custom Monitors, refer to **Custom Monitors** topic.

### Note
In **Network Deployment mode**, Network Deployer will be listed in the WebSphere Monitors list. Clicking on it, will give server information and the custom attributes. Further, the individual WebSpheres within the Network Deployment would also be listed. Clicking on those servers would bring up each of those server’s details.

### See Also
- Creating New Monitor - WebSphere Server
Database Servers

Applications Manager provides Database Server monitoring that monitors system resources. It also provides proactive measures by notifying database and system administrators about potential problems that could compromise database performance. This database server monitoring has the ability to connect to the database source, process any query received in the database, monitor various system table column values, collect data, etc. and also notify through alerts, if the database system properties are beyond a given threshold.

The different database servers supported are:

- MySQL Database Servers
- Oracle Database Servers
- MS SQL Database Servers
- IBM DB2 Database Servers

Please browse through the different database servers that provide server information and their parameters being monitored.

See Also

Creating New Monitor - Database Server
MySQL DB Servers

Supported Versions

The following versions of the MySQL DB Servers can be monitored by the Applications Manager:

1. MySQL 3.23.x
2. MySQL 4.x, 5.x

Monitored Parameters

This section provides information on the MySQL parameters that are monitored and also the details that you can view in a MySQL Monitor page.

Monitor Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Denotes the name of MySQL server monitor.</td>
</tr>
<tr>
<td>Health</td>
<td>Denotes the health (Clear, Warning, Critical) of the MySQL server.</td>
</tr>
<tr>
<td>Type</td>
<td>Denotes the type you are monitoring.</td>
</tr>
<tr>
<td>MySQL Version</td>
<td>Specifies the version of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port number at which the database server is running.</td>
</tr>
<tr>
<td>Base Directory</td>
<td>Specifies the directory in which the database server is installed.</td>
</tr>
<tr>
<td>Data Directory</td>
<td>Specifies the directory in which the database server is installed.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Specifies the host at which the database server is running.</td>
</tr>
<tr>
<td>Host OS</td>
<td>Specifies the OS of the host where the database server is running.</td>
</tr>
<tr>
<td>Last Alarm</td>
<td>Specifies the last alarm that was generated for the database server.</td>
</tr>
<tr>
<td>Last Polled at</td>
<td>Specifies the time at which the last poll was performed.</td>
</tr>
<tr>
<td>Next Poll at</td>
<td>Specifies the time at which the next poll is scheduled.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
</tbody>
</table>

Connection Time

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Time</td>
<td>Specifies the time taken to connect to the database</td>
</tr>
<tr>
<td>Request Rate</td>
<td>Number of request received in one second.</td>
</tr>
</tbody>
</table>

Requests Statistics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Rate</td>
<td>Number of request received in one second.</td>
</tr>
<tr>
<td>Bytes Received Rate</td>
<td>Number of bytes received in one second.</td>
</tr>
<tr>
<td>Bytes Sent Rate</td>
<td>Number of bytes sent in one second.</td>
</tr>
</tbody>
</table>
**Connection Statistics**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Connections</td>
<td>The number of connections opened at present in the MySQL Server.</td>
</tr>
<tr>
<td>Aborted Connections</td>
<td>Number of tries to connect to the MySQL server that failed.</td>
</tr>
<tr>
<td>Aborted Clients</td>
<td>Number of clients aborted by MySQL server.</td>
</tr>
</tbody>
</table>

**Thread Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threads Used</td>
<td>Number of threads processing the request.</td>
</tr>
<tr>
<td>Threads in Cache</td>
<td>Number of threads currently placed in the thread cache.</td>
</tr>
<tr>
<td>Thread Cache Size</td>
<td>Specifies the cache size in the MySQL server.</td>
</tr>
</tbody>
</table>

**Database Details**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>Name of the database instance.</td>
</tr>
<tr>
<td>Database Size</td>
<td>Size of the various databases in the MySQL server.</td>
</tr>
</tbody>
</table>

**Table Lock Statistics**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate Locks</td>
<td>Number of times a table lock for the table is acquired immediately.</td>
</tr>
<tr>
<td>Locks Wait</td>
<td>Number of times a table lock could not be acquired after waiting.</td>
</tr>
</tbody>
</table>

**Key Efficiency**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Hitrate</td>
<td>Percentage of key read requests that resulted in actual key reads from the key buffer.</td>
</tr>
<tr>
<td>Key Buffer Used</td>
<td>Amount of allocated key buffer in use.</td>
</tr>
<tr>
<td>Key Buffer Size</td>
<td>Size of the buffer used for index blocks. Also known as the key cache.</td>
</tr>
</tbody>
</table>

**Query Cache Hitrate**

*Note:* This performance data is not available for MySQL versions 3.23.x

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Cache Hitrate</td>
<td>Ratio of queries that were cached and queries that were not cached.</td>
</tr>
<tr>
<td>Query Cache Size</td>
<td>Amount of memory allocated for caching query results.</td>
</tr>
<tr>
<td>Query Cache Limit</td>
<td>Maximum amount of memory for storing cache results.</td>
</tr>
</tbody>
</table>

**See Also**

Creating New Monitor - MySQL Database Server
Oracle DB Servers

Supported Versions

Applications Manager supports monitoring of Oracle database servers of versions 8.x, 9i, 10g and RAC (Real Application Clusters)

Monitored Parameters

This section provides information on the Oracle parameters that are monitored and also the details that you can view in a Oracle Monitor page.

Monitor Information

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Oracle server monitor</td>
</tr>
<tr>
<td>Oracle Version</td>
<td>Refers to the Version of the Oracle Database.</td>
</tr>
<tr>
<td>Oracle Start Time</td>
<td>Refers to the time when Oracle server was started.</td>
</tr>
<tr>
<td>Availability</td>
<td>Refers to the status of the database server - available or not available.</td>
</tr>
</tbody>
</table>

Connection Time

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Time</td>
<td>Refers to the time taken to connect to the database.</td>
</tr>
</tbody>
</table>

User Activity

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Users</td>
<td>This refers to the number of users executing an SQL Statement.</td>
</tr>
</tbody>
</table>

Database Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Created Time</td>
<td>Creation time of the database.</td>
</tr>
<tr>
<td>Open Mode</td>
<td>Indicates the Open mode of the Instance which can be either Read Write or Read.</td>
</tr>
<tr>
<td>Log Mode</td>
<td>If the transactions are written on the Log, the Log mode will be ARCHIVELOG , or else, the Log mode will be NOARCHIVELOG.</td>
</tr>
</tbody>
</table>
**Database Status**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Size</td>
<td>Size of the database in Megabytes.</td>
</tr>
<tr>
<td>Average Executions</td>
<td>This is the average number of executions that happen during the execution of every SQL Statement.</td>
</tr>
<tr>
<td>Reads</td>
<td>Refers to the number of reads from the database.</td>
</tr>
<tr>
<td>Writes</td>
<td>Refers to the number of writes to the database.</td>
</tr>
<tr>
<td>Block Size</td>
<td>This refers to the lowest possible storage area for an Instance in bytes.</td>
</tr>
</tbody>
</table>

**Table Space Details**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Refers to the name of the Table space.</td>
</tr>
<tr>
<td>Allocated Bytes</td>
<td>Refers to the size of the Table space in bytes.</td>
</tr>
<tr>
<td>Allocated Blocks</td>
<td>Refers to the number of allocated blocks in Table space.</td>
</tr>
<tr>
<td>Data Files</td>
<td>Refers to the number of data files in Table space.</td>
</tr>
</tbody>
</table>

**Table Space Status**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Refers to the name of the Table space.</td>
</tr>
<tr>
<td>Status</td>
<td>Tablespace status: ONLINE, OFFLINE, or INVALID (tablespace has been dropped)</td>
</tr>
<tr>
<td>Free Bytes</td>
<td>Refers to the available free space in bytes.</td>
</tr>
<tr>
<td>Free Blocks</td>
<td>Refers to the number of free blocks in Table space.</td>
</tr>
<tr>
<td>Reads</td>
<td>Refers to the number of reads from the Table space.</td>
</tr>
<tr>
<td>Writes</td>
<td>Refers to the number of writes on the Table space.</td>
</tr>
<tr>
<td>Read Time</td>
<td>Time taken for a single read from the Table space.</td>
</tr>
<tr>
<td>Write Time</td>
<td>Time taken for a single write on the Table space.</td>
</tr>
</tbody>
</table>

**SGA Details**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Cache Size</td>
<td>The total size of the Buffer Cache given in bytes.</td>
</tr>
<tr>
<td>Shared Pool Size</td>
<td>The size of the shared pool given in bytes.</td>
</tr>
<tr>
<td>Redolog Buffer Size</td>
<td>The size of the buffers for the Redo Logs in bytes.</td>
</tr>
<tr>
<td>Library Cache Size</td>
<td>The size of the Library Cache given in bytes.</td>
</tr>
<tr>
<td>Data Dictionary Cache Size</td>
<td>The cache size of the data dictionary or row cache in bytes.</td>
</tr>
<tr>
<td>SQL Area Size</td>
<td>The size of the SQL Area for usage of SQL/PL statements (bytes).</td>
</tr>
<tr>
<td>Fixed Area Size</td>
<td>The size of the SGA, which is fixed throughout the instance.</td>
</tr>
</tbody>
</table>
SGA Status

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Hit Ratio</td>
<td>When a scan of the buffer cache shows that there are no free buffers, Database Block Writer determines which blocks to be eliminated based on a least recently used algorithm or LRU. Having a block required by a user process in the buffer cache already is called a buffer cache hit or is determined as a ratio. Hits are good because they reduce the amount of disk I/O required for the user process.</td>
</tr>
<tr>
<td>Data Dictionary Hit Ratio</td>
<td>The purpose of the row or dictionary cache is to store rows of information from the data dictionary in memory for faster access. The row cache is designed to hold the actual rows of data from objects in data dictionary. While this data is held in the row cache, the users of the database may access that information more quickly than if Oracle had to read the data into memory from disk. The ratio of the data gets to the data misses in the row cache is Data Dictionary Hit Ratio.</td>
</tr>
<tr>
<td>Library Hit Ratio</td>
<td>The Library cache stores all shared SQL and PL/SQL blocks, along with their parse trees. In OLTP environments where a large numbers of users are entering and exchanging data, there is a great chance for overlapping the parse and execute needs of those different queries. Such an overlap in the library is called a cache hit and the ratio determined to the misses and hits is called Library Cache Hit Ratio.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Refers to the size of the free memory in bytes.</td>
</tr>
</tbody>
</table>

Performance of Data Files

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data File Name</td>
<td>Name and location of the data file.</td>
</tr>
<tr>
<td>Table Space Name</td>
<td>Name of the Table space.</td>
</tr>
<tr>
<td>Status</td>
<td>If a data file is a part of the system table space, its status is SYSTEM (unless it requires recovery). If a data file in a non-SYSTEM table space is online, its status is ONLINE. If a data file in non-SYSTEM table space is offline, its status can be either OFFLINE OR RECOVER.</td>
</tr>
<tr>
<td>Created Bytes</td>
<td>Size of the Data file in bytes.</td>
</tr>
<tr>
<td>Reads</td>
<td>Refers to the number of reads from the Data file.</td>
</tr>
<tr>
<td>Writes</td>
<td>Refers to the number of writes to the Data file.</td>
</tr>
<tr>
<td>Average Read Time</td>
<td>Refers to the average read time.</td>
</tr>
<tr>
<td>Average Write Time</td>
<td>Refers to the average write time.</td>
</tr>
</tbody>
</table>
Session Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Session Identifier for the connected session.</td>
</tr>
<tr>
<td>Status</td>
<td>Current status: ONLINE, OFFLINE, or INVALID (tablespace has been dropped).</td>
</tr>
<tr>
<td>Machine</td>
<td>Name of the operating system user.</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of the Oracle process user.</td>
</tr>
<tr>
<td>Elapsed Time</td>
<td>Time elapsed in seconds after which the user has logged into the oracle server.</td>
</tr>
<tr>
<td>CPU Used</td>
<td>CPU centiseconds (divide by 100 to get real CPU seconds) used by this session.</td>
</tr>
<tr>
<td>Memory Sorts</td>
<td>Number of memory sorts performed.</td>
</tr>
<tr>
<td>Table Scans</td>
<td>Number of table scans performed.</td>
</tr>
<tr>
<td>Physical Reads</td>
<td>Physical reads for the session.</td>
</tr>
<tr>
<td>Logical Reads</td>
<td>Sum of consistent gets and db block gets.</td>
</tr>
<tr>
<td>Commits</td>
<td>Number of commits made by user in a second.</td>
</tr>
<tr>
<td>Cursor</td>
<td>Number of cursor currently in use.</td>
</tr>
<tr>
<td>Buffer Cache Hit Ratio</td>
<td>Percentage of session logical reads taking place from the buffer (1-physical reads/session logical reads*100).</td>
</tr>
</tbody>
</table>

Rollback Segment

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Name</td>
<td>Name of the rollback segment.</td>
</tr>
<tr>
<td>Table Space Name</td>
<td>Name of the tablespace containing the rollback segment.</td>
</tr>
<tr>
<td>Status</td>
<td>ONLINE if the segment is online, or PENDING OFFLINE if the segment is going offline but some active (distributed) transactions are using the rollback segment. When the transaction(s) complete, the segment goes OFFLINE.</td>
</tr>
<tr>
<td>Current Size</td>
<td>Current size in bytes of the rollback segment.</td>
</tr>
<tr>
<td>Initial Extent</td>
<td>Initial extent size in bytes.</td>
</tr>
<tr>
<td>Next Extent</td>
<td>Secondary extent size in bytes.</td>
</tr>
<tr>
<td>Min. Extent</td>
<td>Minimum number of extents.</td>
</tr>
<tr>
<td>Max. Extent</td>
<td>Maximum number of extents.</td>
</tr>
<tr>
<td>Hit Ratio</td>
<td>Ratio of gets to waits. This should be &gt;= 99%.</td>
</tr>
<tr>
<td>HWMSIZE</td>
<td>High Water Mark of rollback segment size.</td>
</tr>
<tr>
<td>Shrinks</td>
<td>Number of times rollback segment shrank, eliminating one or more additional extents each time.</td>
</tr>
<tr>
<td>Wraps</td>
<td>Number of times rollback segment wraps from one extent to another.</td>
</tr>
<tr>
<td>Extend</td>
<td>Number of times rollback segment was extended to have a new extent.</td>
</tr>
</tbody>
</table>

See Also

Creating New Monitor - Oracle Database Server
MS SQL DB Servers

Supported Versions
Applications Manager supports monitoring of MS SQL 2000 and 2005 versions.

Monitored Parameters
This section provides information on the MS SQL parameters that are monitored and also the details that you can view in a MS SQL Monitor page.

Monitor Information

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of MS SQL server monitor.</td>
</tr>
<tr>
<td>Health</td>
<td>Specifies the health (Clear, Warning, Critical) of the MS SQL server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type you are monitoring.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port number at which the database server is running.</td>
</tr>
<tr>
<td>ODBC Driver Version</td>
<td>Specifies the ODBC driver version used.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Specifies the host at which the database server is running.</td>
</tr>
<tr>
<td>Host OS</td>
<td>Specifies the OS of the host where the database server is running.</td>
</tr>
<tr>
<td>Last Alarm</td>
<td>Specifies the last alarm that was generated for the database server.</td>
</tr>
<tr>
<td>Last Polled at</td>
<td>Specifies the time at which the last poll was performed.</td>
</tr>
<tr>
<td>Next Poll at</td>
<td>Specifies the time at which the next poll is scheduled.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
</tbody>
</table>

Memory Usage

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Memory</td>
<td>Total amount of dynamic memory the server is currently consuming.</td>
</tr>
<tr>
<td>SQL Cache Memory</td>
<td>Total amount of dynamic memory the server is using for the dynamic SQL cache.</td>
</tr>
<tr>
<td>Lock Memory</td>
<td>Total amount of dynamic memory the server is using for locks.</td>
</tr>
<tr>
<td>Optimizer Memory</td>
<td>Total amount of dynamic memory the server is using for query optimization.</td>
</tr>
<tr>
<td>Connection Memory</td>
<td>Total amount of dynamic memory the server is using for maintaining connections.</td>
</tr>
<tr>
<td>Granted WorkSpace Memory</td>
<td>Total amount of memory granted to executing processes. This memory is used for hash, sort and create index operations.</td>
</tr>
<tr>
<td>Memory Grants Pending</td>
<td>Current number of processes waiting for a workspace memory grant.</td>
</tr>
<tr>
<td>Memory Grants Success</td>
<td>Current number of processes that have successfully acquired a workspace memory grant.</td>
</tr>
</tbody>
</table>
### Buffer Manager Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Hit Ratio</td>
<td>Percentage of pages that were found in the buffer pool without having to incur a read from disk.</td>
</tr>
<tr>
<td>Page LookUps/Min</td>
<td>Number of requests to find a page in the buffer pool.</td>
</tr>
<tr>
<td>Page Reads/Min</td>
<td>Number of physical database page reads issued.</td>
</tr>
<tr>
<td>Page Writes/Min</td>
<td>Number of physical database page writes issued.</td>
</tr>
<tr>
<td>Total Pages</td>
<td>Number of pages in the buffer pool (includes database, free, and stolen).</td>
</tr>
<tr>
<td>Database Pages</td>
<td>Number of pages in the buffer pool with database content.</td>
</tr>
<tr>
<td>Free Pages</td>
<td>Total number of pages on all free lists.</td>
</tr>
</tbody>
</table>

### Connection Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Time</td>
<td>Time taken to get connected to the MS SQL database server.</td>
</tr>
<tr>
<td>Active Connections</td>
<td>Number of users connected to the system.</td>
</tr>
<tr>
<td>Logins/Min</td>
<td>Total number of logins started per minute.</td>
</tr>
<tr>
<td>Logouts/Min</td>
<td>Total number of logouts started per minute.</td>
</tr>
</tbody>
</table>

### Cache Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Hit Ratio</td>
<td>Ratio between cache hits and lookups</td>
</tr>
<tr>
<td>Cache Used/Min</td>
<td>Times each type of cache object has been used</td>
</tr>
<tr>
<td>Cache Count</td>
<td>Number of cache objects in the cache</td>
</tr>
<tr>
<td>Cache Pages</td>
<td>Number of 8k pages used by cache objects</td>
</tr>
</tbody>
</table>

### Lock Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Requests/Min</td>
<td>Number of new locks and lock conversions requested from the lock manager.</td>
</tr>
<tr>
<td>Lock Waits/Min</td>
<td>Total wait time for locks in the last minute.</td>
</tr>
<tr>
<td>Lock Timeouts/Min</td>
<td>Number of lock requests that timed out. This includes internal requests for NOWAIT locks.</td>
</tr>
<tr>
<td>Deadlocks/Min</td>
<td>Number of lock requests that resulted in a deadlock.</td>
</tr>
<tr>
<td>Average Lock Wait Time</td>
<td>The average amount of wait time for each lock request that resulted in a wait.</td>
</tr>
</tbody>
</table>
SQL Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Requests/Min</td>
<td>Number of SQL batch requests received by server.</td>
</tr>
<tr>
<td>SQL Compilations/Min</td>
<td>Number of SQL compilations.</td>
</tr>
<tr>
<td>SQL Recompilations/Min</td>
<td>Number of SQL re-compiles.</td>
</tr>
<tr>
<td>AutoParams/Min</td>
<td>Number of auto-parameterization attempts.</td>
</tr>
<tr>
<td>Failed AutoParams/Min</td>
<td>Number of failed auto-parameterizations.</td>
</tr>
</tbody>
</table>

Latch Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latch Waits/Min</td>
<td>Number of latch requests that could not be granted immediately and had to wait before being granted.</td>
</tr>
<tr>
<td>Average Latch Wait Time</td>
<td>Average latch wait time for latch requests that had to wait.</td>
</tr>
</tbody>
</table>

Access Method Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Scans/Min</td>
<td>Number of unrestricted full scans. These can either be base table or full index scans.</td>
</tr>
<tr>
<td>Range Scans/Min</td>
<td>Number of qualified range scans through indexes.</td>
</tr>
<tr>
<td>Probe Scans/Min</td>
<td>Number of probe scans. A probe scan is used to directly look up rows in an index or base table.</td>
</tr>
</tbody>
</table>

Database Details

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataFile Details</td>
<td>Gives the DataFile size.</td>
</tr>
<tr>
<td>Log File Size</td>
<td>Gives the Size of the Log File, used size of the Log File.</td>
</tr>
<tr>
<td>Transaction Details</td>
<td>Gives the number of transaction per minute, replication transaction per minute, and the active transactions.</td>
</tr>
<tr>
<td>Log Flush Details</td>
<td>Gives the number of Log Flush/minute, Log Flush waits/minute, and the Log Flush wait time.</td>
</tr>
</tbody>
</table>

See Also

Creating New Monitor - MS SQL Database Server
IBM DB2 DB Servers

Supported Versions

Applications Manager supports monitoring of IBM DB2 8.x versions.

Monitored Parameters

This section provides information on the IBM DB2 parameters that are monitored and also the details that you can view in a DB2 Monitor details page.

Monitor Information

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of IBM DB2 server monitor.</td>
</tr>
<tr>
<td>Health</td>
<td>Specifies the health (Clear, Warning, Critical) of the IBM DB2 server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type you are monitoring.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port number at which the database server is running.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>The name of the instance in which the database is present</td>
</tr>
<tr>
<td>Server Status</td>
<td>The current status of the database server itself</td>
</tr>
<tr>
<td>Started Time</td>
<td>The date and time that the database manager was started using the db2start command</td>
</tr>
<tr>
<td>Host Name</td>
<td>Specifies the host at which the database server is running.</td>
</tr>
<tr>
<td>Host OS</td>
<td>Specifies the OS of the host where the database server is running.</td>
</tr>
<tr>
<td>Last Alarm</td>
<td>Specifies the last alarm that was generated for the database server.</td>
</tr>
<tr>
<td>Last Polled at</td>
<td>Specifies the time at which the last poll was performed.</td>
</tr>
<tr>
<td>Next Poll at</td>
<td>Specifies the time at which the next poll is scheduled.</td>
</tr>
<tr>
<td>Availability</td>
<td>Shows the current status of the server - available or not available.</td>
</tr>
</tbody>
</table>

Connection Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Time</td>
<td>Time taken to get connected to the IBM DB2 database server</td>
</tr>
<tr>
<td>Total Connections</td>
<td>The total number of local and remote connections that currently present in the database manager</td>
</tr>
<tr>
<td>Local Connections</td>
<td>The number of connections initiated from remote clients to the current instance of the database manager</td>
</tr>
<tr>
<td>Remote Connections</td>
<td>The number of local applications that are currently connected to the database within the database manager</td>
</tr>
</tbody>
</table>
### Agents Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Agents</td>
<td>The number of agents in the agent pool that are currently active and assigned to an application</td>
</tr>
<tr>
<td>Idle Agents</td>
<td>The number of agents in the agent pool that are currently unassigned to any application</td>
</tr>
<tr>
<td>Number of Agents</td>
<td>The number of agents registered in the current database manager instance</td>
</tr>
<tr>
<td>Agents Waiting</td>
<td>The number of agents waiting for a token so they can execute a transaction in the database manager</td>
</tr>
</tbody>
</table>

### Database Information

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>The real name of the database for which information is collected</td>
</tr>
<tr>
<td>Health</td>
<td>Specifies the health (Clear, Warning, Critical) of the database.</td>
</tr>
<tr>
<td>Database Alias</td>
<td>The alias of the database provided when calling the snapshot function</td>
</tr>
<tr>
<td>Database Path</td>
<td>The full path of the location where the database is stored on the monitored system</td>
</tr>
<tr>
<td>Database Status</td>
<td>The current status of the database</td>
</tr>
<tr>
<td>Connected Time</td>
<td>The date and time when the activate database was issued</td>
</tr>
<tr>
<td>Deadlock Rate</td>
<td>The total number of deadlocks that have occurred in the given polling interval</td>
</tr>
<tr>
<td>Percentage of Log Utilization</td>
<td>The total amount of active log space used in bytes in the database</td>
</tr>
<tr>
<td>Percentage of Sorts Overflowed</td>
<td>The percentage of sorts that have over flowed</td>
</tr>
</tbody>
</table>

### Transaction Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Queries</td>
<td>The total number of successful SQL statements executed at the database in the given polling interval</td>
</tr>
<tr>
<td>Failed Queries</td>
<td>The number of SQL statements that were attempted, but failed at the database in the given polling interval</td>
</tr>
<tr>
<td>Units of Work</td>
<td>This represents the total number of sql commits, internal commits, sql roll backs and internal roll backs done by the database manager in the given polling interval</td>
</tr>
</tbody>
</table>
Cache Performance

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Cache Hit Ratio</td>
<td>The hit ratio is a percentage indicating how well the package cache is helping to avoid reloading packages and sections for static SQL from the system catalogs as well as helping to avoid recompiling dynamic SQL statements.</td>
</tr>
<tr>
<td>Catalog Cache Hit Ratio</td>
<td>The hit ratio is a percentage indicating how well the catalog cache is helping to avoid actual accesses to the catalog on disk.</td>
</tr>
</tbody>
</table>

Buffer Statistics

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Pool Hit Ratio</td>
<td>The buffer pool hit ratio indicates the percentage of time that the database manager loaded the required page from buffer pool in order to service a page request</td>
</tr>
<tr>
<td>Index Page Hit Ratio</td>
<td>The Index Page hit ratio indicates the percentage of time that the database manager accessed the index pages present in the buffer pools.</td>
</tr>
<tr>
<td>Data Page Hit Ratio</td>
<td>The Data Page hit ratio indicates the percentage of time that the database manager accessed the data pages present in the buffer pools.</td>
</tr>
<tr>
<td>Direct Reads</td>
<td>The number of read operations that do not use the buffer pool</td>
</tr>
<tr>
<td>Direct Writes</td>
<td>The number of write operations that do not use the buffer pool</td>
</tr>
</tbody>
</table>

See Also

Creating New Monitor - IBM DB2 Database Server
Services

Applications Manager supports monitoring of the following Services to check their status:

- JMX [MX4J / JDK 1.5]
- Service Monitoring
- AdventNet JMX Agent - RMI Adapter
- SNMP
- Telnet

It performs the following checks to ensure its availability and represents the information in the form of graphs. Click on the Monitor of the Monitor Group to view the graphical representation of its data and also the details of its parameters.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMX [MX4J / JDK 1.5]</td>
<td>• Connects to the MX4J-JMX agent to check availability and response time of RMI Connector. You can also view the custom attributes of the MX4J-JMX agent in the same page. Further, alerts can be generated for JMX notifications through JMX Notification Listener. For information on adding Custom Monitors, refer to Custom Monitors topic.</td>
</tr>
</tbody>
</table>
| Service Monitoring | • Monitors different services running in particular/default ports such as FTP-21, Telnet-23 etc running in the network.  
• Connects to the server configured for monitoring. 
• Checks availability and the response time of the service. Here, the response time is the time taken to connect to the port, execute the given command and search the string. |
| AdventNet JMX Agent- RMI Adapter | • Connects to the AdventNet JMX agent to check availability and performance of RMI Adapter. You can also view the custom attributes of the JMX agent in the same page. For information on adding Custom Monitors, refer to Custom Monitors topic. |
| SNMP | • Connects to SNMP agent running in an application and monitors the availability and performance of the service. You can also view the custom attributes of the SNMP agent in the same page. For information on adding Custom Monitors, refer to Custom Monitors topic. |
| Telnet | • Connects to Telnet port (default 23) and checks its availability. 
• Monitors response time and updates the status based on a given threshold. |

See Also

Creating New Monitor - Services
Mail Servers

Applications Manager supports monitoring of the following Mail Servers

- Exchange Server
- Mail Server

It performs the following checks to ensure its availability and represents the information in the form of graphs. Click on the Monitor of the Monitor Group to view the graphical representation of its data and also the details of its parameters.

Exchange Server

- Connects to system in which Exchange Server is running, to check availability of the Exchange Server. Checks for the availability of the following services:
  - MS Exchange Information Store
  - MS Exchange Site Replication Store
  - MS Exchange MTA Stacks
  - MS Exchange Management
  - SMTP
  - POP3
  - IMAP4
  - MS Exchange System Attendant
  - MS Exchange Routing Engine
  - MS Exchange Event Service

- You can view the performance data as attributes of the system via reports and graphs. The following table gives the various data that is being monitored:

<table>
<thead>
<tr>
<th>SMTP Connections</th>
<th>Inbound Connections</th>
<th>Outbound Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Transfer Agent Connections</td>
<td>Inbound Associations</td>
<td>Outbound Associations</td>
</tr>
<tr>
<td>POP &amp; IMAP Connections</td>
<td>POP Connections</td>
<td>IMAP Connections</td>
</tr>
<tr>
<td>Information Store Connections &amp; Users</td>
<td>Active Connections</td>
<td>Active Users</td>
</tr>
<tr>
<td>SMTP Stats</td>
<td>Local Retry Queue Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote Retry Queue Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote Queue Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Pending Routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages in Local Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Currently Undeliverable Messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Categorizer Queue Length</td>
<td></td>
</tr>
<tr>
<td>MTA Stats</td>
<td>Work Queue Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Message Bytes Per Sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP/IP Received Bytes Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP/IP Transmit Bytes Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Recipients Queued</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Work Queue Bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Queue Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Queued Bytes</td>
<td></td>
</tr>
<tr>
<td>Information Store Stats</td>
<td>Messages from MTA to IS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages from IS to MTA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Pending Local Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Received Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Sent Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HSOT Cache Hits</td>
<td></td>
</tr>
<tr>
<td>Information Store</td>
<td>Receive Queue Size</td>
<td></td>
</tr>
<tr>
<td>Mailbox Stats</td>
<td>Send Queue Size</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Delivered Per min</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Sent Per min</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logon Operations Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used Disk Space</td>
<td></td>
</tr>
<tr>
<td>Directory &amp; Event Service Stats</td>
<td>Pending Replication Synchronizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remaining Replication Updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notify Queue</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AddressLists Queue Length</td>
<td></td>
</tr>
<tr>
<td>Information Store Public Folder Stats</td>
<td>Receive Queue Size</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send Queue Size</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Delivered Per min</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Messages Sent Per min</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logon Operations Per sec</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used Disk Space</td>
<td></td>
</tr>
</tbody>
</table>

**Mail Server**
- Connects to the Mail Server and performs both SMTP and POP operations.
- Checks both SMTP and POP servers to ensure **availability**.
- Enables performance management by monitoring the **response time** of the server and updates the status based on a given threshold.

**See Also**

Creating New Monitor - Mail Servers
Web Services

Applications Manager supports monitoring of the following Web Services to check their status:

- Apache Server
- IIS Server
- PHP
- Web Server
- HTTP - URLs and HTTP - URL Sequence

It performs the following checks to ensure its availability and represents the information in the form of graphs. Click on the Monitor of the Monitor Group to view the graphical representation of its data and also the details of its parameters.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Checks</th>
</tr>
</thead>
</table>
| Apache Server | - Connects to the Apache and checks its availability and response time.  
- When Server Status and Extended Status are enabled, then the following data can be obtained.  
  1. Total Accesses  
  2. Total KBs  
  3. CPU Load  
  4. Uptime  
  5. ReqPerSec  
  6. BytesPerSec  
  7. BytesPerReq  
  8. BusyWorkers  
  9. IdleWorkers  
- To Enable the Server Status, follow the steps given below:  
  1. In Apache's httpd.conf file, locate "Location /server-status" tag.  
  2. Remove the comment in the Location/Server-status tag, to Enable SetHandler server-status  
  3. Change the attribute "deny from all" to "Allow from all"  
  4. Remove the comment in "LoadModule status_module modules/mod_status.so".  
  5. Save the conf file and restart the Apache Server  
- To enable the Extended-status, follow the steps given below:  
  2. Remove the comment to enable the status.  
  3. Save the conf file and restart the Apache Server |
| IIS Server | - Connects to the IIS server and checks its availability.  
- Monitors response time and updates the status based on a given threshold. |
<table>
<thead>
<tr>
<th>Service Type</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP Monitoring</td>
<td>• Connects to the server and retrieves PHP and checks its availability.</td>
</tr>
<tr>
<td></td>
<td>• Monitors response time and updates the status based on a given threshold.</td>
</tr>
<tr>
<td></td>
<td>• In Linux, Page fault of the system in which the PHP is hosted is also shown. We can configure the alert and actions based on the threshold condition.</td>
</tr>
<tr>
<td>Web Server</td>
<td>• Connects to the web server and checks its availability.</td>
</tr>
<tr>
<td></td>
<td>• Monitors response time and updates the status based on a given threshold.</td>
</tr>
</tbody>
</table>

**Troubleshoot Apache Server**: If you are not able to view the data even after enabling the Server Status and Extended Status, kindly ensure that `http://hostname:portno/server-status?auto` gives the required data.

### See Also

*Creating New Monitor - Web Services*
Servers

In Network-level management, maintaining the status and connectivity of the network, is a picture at a higher level. It is of prime importance to know the status of the machines in the network, how loaded (or overloaded) they are and how efficiently they are utilized (or overused) to enable necessary corrective administrative functions to be performed on the identified overloaded/poorly performing systems.

Server-level management is a down-to-earth concept which involves lot of manual intervention, human resources, and administrative tasks to be performed. Applications Manager provides with a Server-level monitoring functionality to achieve such goals and to ease the process of configuration management of hosts.

Supported Operating Systems

1. Windows
2. Linux
3. Sun Solaris
4. IBM AIX
5. HP Unix
6. Tru64 Unix
7. FreeBSD

Monitored Parameters

The following are the parameters that are represented graphically based on the current values.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Load</td>
<td>Specifies the number of jobs handled by the system in 1/ 5/ 15 minutes with its peak and current value, and current status.</td>
</tr>
<tr>
<td>Disk Utilization</td>
<td>Specifies the hard disk space utilized by the system and updates with the peak and current value, and current status of the Disk Partition parameter.(The parameter includes C, D, E, F drives, etc. in windows, /home, etc. in Linux.)</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Swap Memory Utilization: Specifies the swap space or the virtual memory utilized by the system with peak and current value, and current status of the parameter. Physical Memory Utilization: Specifies the amount of physical memory utilized by the system with peak and current value, and current status of the parameter.</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Specifies the total CPU used by the system with its peak and current value, and current status.</td>
</tr>
</tbody>
</table>

The following table briefs the parameters monitored by the respective Servers.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization.</td>
</tr>
<tr>
<td>Windows NT</td>
<td>Disk Utilization and Memory Utilization</td>
</tr>
<tr>
<td>Windows 2003, XP</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization.</td>
</tr>
<tr>
<td>Linux</td>
<td>System Load, Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring includes Telnet, SSH, and SNMP).</td>
</tr>
<tr>
<td>Sun Solaris</td>
<td>System Load, Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring includes Telnet, SSH, and SNMP).</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring</td>
</tr>
</tbody>
</table>
### Operating System Parameters

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Unix</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring includes Telnet and SSH)</td>
</tr>
<tr>
<td>Tru64 Unix</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring includes Telnet and SSH)</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>Disk Utilization, Memory Utilization, and CPU Utilization (mode of monitoring includes Telnet, SSH, and SNMP)</td>
</tr>
</tbody>
</table>

**Note:** To know more about the configuration details required while discovering the host resource, click [here](#).

### Process Monitoring

Apart from the above mentioned parameters, you can also monitor the processes running in a server.

#### To monitor processes in a server

1. In the Server Monitor page (which displays details of CPU Utilization, Memory Utilization, etc.), under **Process Details**, click **Add New Process**.
2. All the processes that are running would be displayed along with CPU and Memory utilization statistics. (Only memory statistics is shown for Windows and SNMP mode of monitoring)
3. Select the processes that you want to monitor.

After configuring the processes, they are listed under the **Process Details** section of the Server Monitor page. By clicking on the process, you can view its availability graph. You can also configure alerts for a particular process.

You can edit the Display Name, Process Name, Commands and Arguments of the particular process by clicking on the Edit Process icon.

### Associating Scripts and URLs to the Host Resource:

By associating a script or a URL to a Host resource, their attributes become one among the other attributes of the Host and their data is also shown under Host Details itself. Health of the Host resource is dependent on the Health of the Scripts and URLs aswell.

For eg., If you wish to monitor RequestExecutionTime, RequestsCurrent, RequestsDisconnected of the ASP.NET application, WMI scripts can be used to get the statistics (this info is not available when Applications Manager is used). You can write your own script that would fetch these details then configure this script to the Applications Manager. After configuring this script to the Applications Manager you can associate this script to the Host monitor itself. Then the attributes of the script would behave like the other attributes of the Host monitor. Hence, you can configure in such a way that the Health of the script directly affects the Health of the host.

Likewise, If you want to monitor a website hosted in a system in such a way that, whenever there is a change in the health of the website, the health of the server should reflect the change. In this case you can configure the url monitor and then associate that url to the host. Hence, if the website is down, the health of the Host resource is affected.

- **Associate/Remove Scripts:** Click on ‘Associate/Remove Scripts’ link in Host Details. Scripts that are associated and that are not associated with the Host would be listed. Accordingly, you can then select the scripts that you want to associate or remove.
• **Associate/Remove URLs**: Click on 'Associate/Remove URLs' link in Host Details. URLs that are associated and that are not associated with the Host would be listed. Accordingly, you can then select the URLs that you want to associate or remove.

**See Also**

Creating New Monitor - Servers
HTTP URL Monitors

Applications Manager acts as a continuous URL monitoring service that keeps a constant watch over the specified URL or web site pages. URL monitors verify the availability of specified, addressable, standard HTTP and HTTPS URLs. They scan the HTTP and HTTPS pages looking for a predefined keyword to check whether the web site is available.

There are two ways of URL monitoring provided by Applications Manager.

- URL Monitoring
- URL Sequence

In URL Sequence, click on the individual URL listed, to view its monitored parameters.

Monitored Parameters

The following parameters are monitored for URL Monitors (both URL Monitoring and URL Sequence):

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Information</td>
<td></td>
</tr>
<tr>
<td>Health</td>
<td>Specifies the health of the monitor based on its dependencies.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of Monitoring</td>
</tr>
<tr>
<td>URL address</td>
<td>Specifies the URL being monitored</td>
</tr>
<tr>
<td>Match Content</td>
<td>The string that is searched in the resulting html page.</td>
</tr>
<tr>
<td>Request Method</td>
<td>The request method sent to the HTTP/HTTPS URL (Get or Post)</td>
</tr>
<tr>
<td>Monitored Parameters</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td>The current status of the URL / URL Sequence- whether it is up or down.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The response time for accessing an URL or total response time of URL Sequence</td>
</tr>
<tr>
<td>Current Status</td>
<td>Current status of the response time. Click on the icon to know its RCA details.</td>
</tr>
<tr>
<td>Current Page Size</td>
<td>The current page size of the URL in bytes (only in URL monitoring)</td>
</tr>
<tr>
<td>% Change in Page Size</td>
<td>The % change between the current page size and the previous page size. (only in URL monitoring)</td>
</tr>
</tbody>
</table>

See Also

Creating New Monitor - URL Monitors
Custom Monitors

Custom Monitors available are

- JMX / SNMP Dashboard
- Script Monitors
- QEngine Script Monitors

JMX / SNMP Dashboard

These custom monitors provide a real-time, correlated view of the entire application stack improving J2EE/J2SE application performance by monitoring its data sources such as JMX MBean source and SNMP Agents.

JMX / SNMP Dashboard is a logical grouping that consist of data sources such as JMX MBean and SNMP OID. It can have both the JMX and SNMP attributes. Building JMX / SNMP Dashboard involves

- Creating JMX / SNMP Dashboard and adding it to a specific Monitor Group
- Adding Attributes

The advantage of creating the dashboard is to monitor various data source at a common place.

Adding Attributes

Once you add a JMX / SNMP Dashboard, the Add Attributes option is available. Click that to add custom attributes to your Custom Monitor. The following are the data source for which custom monitors are built by Applications Manager. Click on the topics to view the steps required to add the respective data sources or attributes to the Custom Monitor.

- Adding JMX MBean Attributes.
- Adding SNMP OID Attributes.

See Also

Creating New Monitor - Custom Monitors
Adding JMX MBeans Attributes

The following are the JMX MBean resources whose MBean attributes are monitored by Applications Manager using Custom Monitor:

- AdventNet JMX Agent- RMI Adapter
- JMX [MX4J / JDK 1.5]
- WebLogic Server
- JBoss Server
- WebSphere Server

To add the attributes, follow these steps:

1. In the Add Attributes screen, select the JMX MBean resource from the combo box and click Add. You can also discover a resource using Add Monitor provided alongside the combo box and add them to the list of resources.

2. Select the domains and click Show MBeans to list all the MBeans of those domains. You can also specify some filter criteria to match the MBean names. Alternatively, you can add the MBean attributes directly, by choosing the Add the MBean attributes directly option. You can enter the MBean ObjectName, Attribute Name and Attribute Type (String / Numeric) and then add that attribute to be monitored.

3. On clicking Show MBeans button, you get the list of all the MBeans. Select the MBean (all attributes) or only the required attribute(s) by enabling the check box provided alongside. In case of tabular MBeans, select the attribute (all columns) or only the required columns.

4. Click Add Attributes. All the selected attributes will be listed with their details. Note: You have an option to enable / disable reports for scalar numerical attributes, which is indicated through the above images in the Reports column. Refer to Viewing Reports for more details on report generation.

5. Click the Back to Details Page button to view the newly created Custom Monitor. This screen lists all the attributes added.

6. If you want to add or delete attributes, click Add or Delete Custom Attributes.

Note: If the JMX data source is WebLogic Server 6.1 or WebLogic 6.1 sp1, you have to specify the full object name in the filter criteria to get the MBean attributes. This is because of the implementation bug in WebLogic 6.1.

However, versions WebLogic 6.1 SP2 and above do not have this problem.

Note: Steps to Create JMX Notification Listener (JMX [MX4J / JDK 1.5])

- In the JMX [MX4J / JDK 1.5] Monitor page, click on the 'Create new JMX Notification Listener' link.
- The first step is to choose the Domain of the JMX Agent. After selecting the Domain, click on 'Show MBeans' to view the MBeans that belong to the selected Domain.
- The second step is to choose the MBeans from the list that is shown.
- The third step will be to create the new JMX Notification Listener. Enter the Name and select the status of the Listener as enabled or disabled. Set the severity of the Alert that will be generated once a JMX notification is received, as Critical/Warning/Clear. Associated actions that need to be executed when the notification is received can be chosen from the list of actions configured.
- Clicking on 'Save' will have a JMX Notification Listener configured, which would generate Alerts of the configured severity and execute actions.
See Also

- Create New Monitor - AdventNet JMX Agent - RMI Adaptor
- Create New Monitor - JMX [MX4J / JDK 1.5]
- Create New Monitor - WebLogic Server
- Create New Monitor - JBoss Server
- Create New Monitor - WebSphere Server
Adding SNMP OID Attributes

Once the Custom Monitor is created, you have to add the required SNMP attributes added to it. Follow these steps:

1. In the Add Attributes page, select the resource (SNMP Agent data source) from the combo box and click Add. You can also discover a resource from here and add it to the combo box of resource. To do this, refer to Create New Monitor - SNMP Agent section.

2. Provide the following details to add SNMP attributes:
   - **Attribute Display Name**: Provide any name for the attribute.
   - **SNMP Object Identifier**: Provide the OID of the SNMP attribute or browse through the MIB Browser to provide the same. Please go through Working with MIB Browser to know more details on using the MIB Browser.
   - **Attribute Type**: Select the type of the attribute, i.e. Simple (SNMP Scalar) or Table.

3. Click Add SNMP OIDs to add the SNMP OID attribute. All the selected attributes will be listed with their details.

4. Click on Back to Details Page to view the attribute details. This lists all the attributes added to the Custom Monitor, their values, data collection time of the resource, and their associated actions, if any.

5. If you want to add or delete attributes, click Add Attributes or Delete Attributes or Add or Delete Custom Attributes.

Working with MIB Browser

You can use the MIB Browser tool to provide the OID of the SNMP attribute that you want to add to the Custom Monitor. This shows the MIB Browser UI.

Please follow the steps to add the OID of an SNMP attribute:

1. Load the MIB that contains the attribute to be added to the Custom Monitor, using the Load MIB option. A dialog pops up listing all the MIBs present under the <Applications Manager Home>/mibs directory of Applications Manager. By default, the MIB Browser loads the RFC1213 MIB.
2. Choose the MIB and click **Load** to load the selected MIB. The MIBs are listed in the left frame of the MIB Browser UI. Additionally, the MIBs are listed in the combo box of **Loaded Mibs** in the right frame. You can use **Load selected MIB to tree** to choose from the listed MIBs.

3. Browse through the MIB and select the managed information or the SNMP attribute. Its details are displayed on the right frame.

4. You have two options of adding OID(s).
   1. To add all the OIDs under a node, click the node and click **Set OID to screen** button. **Example:** In RFC1213 MIB, click 'systems' node and click **Set OID to screen** button. This adds all the OIDs under 'systems' such as sysDescr, sysObjectID sysUpTime, sysContact, sysName, sysLocation, and sysServices.
   2. To add only a single OID, click that OID on the tree and click **Set OID to screen**. **Example:** Click 'sysDescr' under 'systems' node and click **Set OID to screen** button.

   This adds the OID(s) for the SNMP attribute in the Applications Manager Client.

**Note:**

- The MIB, whose attributes are required to be added to the Custom Monitor, must be present in the `<Applications Manager Home>/working/mibs` directory of Applications Manager. To add the MIBs to the directory, use **Upload Files/Binaries** Form.
- The MIB must be implemented in the SNMP Agent being monitored.
Script Monitors

Applications Manager provides Script Monitoring functionality to manage ad-hoc Windows/Linux scripts that are used in-house.

- During creation of a new script monitor, you need to give the location of the custom script, attributes (numeric/string) to be monitored, the Output File in which the output is going to be redirected and the polling interval.
- Based on the polling interval, Applications Manager executes the script.
- The script will transfer its output to the Output File configured.
- Applications Manager parses the Output File and executes the actions configured.
- Reports for the attributes configured would be shown as graphs. Option to enable or disable reports is given.

Examples:

If you wish to Monitor your Printer Availability through your custom script, find below the steps to follow:

- Write a script (for eg., printerdetails.sh / printerdetails.bat) to check whether the Printer is up or not. This script may inturn execute any class file or exe file and transfer the output to any file say 'output.txt'.
- The attributes that you wish to monitor should be written in the output.txt as key value pair like 'printeravailability=up'. The output delimiter is a single character like "=" or ":". If you don't specify a delimiter, then 'space' would be considered as a delimiter.
- While configuring the script monitor you need to give the output file name with absolute path.
- Attributes should be entered in the expected results field based on their type (String or Number). It is case sensitive
- As per the Polling Interval, Applications Manager will execute the script and the output will be produced in the output.txt
- Thresholds/Action like "Send Email" needs to be configured so that the alerts would be generated based on the values from output.txt file.
- Click on the Script Monitor link in Monitors tab to view the monitor information and the attributes graphs.
- If the printer is down, Applications Manager would monitor the printerdetails.bat and generate an alert by sending an email to the configured email-id.

If you want to monitor the output of the custom script that tracks the paper reserve in the tray, find below an example custom script

- @rem echo off
  @del printoutput.txt
  @echo Name=printername >>printoutput.txt
  @echo PapersinTray=3 >>printoutput.txt
- The output of the above custom script is redirected to an output file called 'printoutput.txt'.
- If the polling interval is say 5 minutes, then for every 5 minutes, the custom script is executed and the results are transferred to 'printoutput.txt' that is generated.
• The printoutput.txt is parsed and the values that were specified to be monitored while creating the script monitor, is displayed and processed.
• Threshold is applied to the values and the corresponding action takes place. If the documents in printer tray is zero then, an email can be sent alerting the same.

See Also
Creating New Monitor - Script Monitors
QEngine Script Monitors

ManageEngine Application Performance Management Solution, integrates both Applications Manager and QEngine to optimize and maintain business critical web applications that meet end user service levels.

ManageEngine Performance Management for the Enterprise provides:

- A complete solution that spans all the way from the quality stage to operations
- A means to ensure application quality before rolling into production. Load testing, functional testing, cross-browser testing are some of the common tests that need to be conducted before a business critical application goes into production.
- Reuse of test scripts recorded during functional testing, in deployment phase.
- Improved application performance and availability management.

Integration of QEngine and Applications Manager

Follow the Steps below, to integrate QEngine Web Performance Test with Application Manager. More info on Web Performance Test is available here

- Record Urls and save the Businesscase. More information on saving the sequence is available here
- Configure the Profile, Workload and Testcase using TestCase Configuration.
- WorkLoad Limitations: Load Type : Normal
  User count: 1
  Test Duration: xxx
  Sample Duration: xxx
  Note: Test Duration and Sample Duration must be equal. Only one sample is allowed. User count should be 1.
- Close the WebPerformance Studio.
- To enable Application Manager integration, Open the file 'CommandLineWebPerfTest.sh/CommandLineWebPerfTest.bat'. Change the variable -DapplicationManager=false as -DapplicationManager=true.
- Edit <QEngine Home>\template\appManagerUrlProps.prop. Modify the value for response_code and response_length from false to true. This will enable monitoring response time, response code and response length. After doing the modification the file will look like given below.
  url=true
  request_start_time=false
  response_time=true
  down_end_time=false
  down_start_time=false
  response_code=true
  response_length=true
- Run CommandLineWebPerfTest.sh/CommandLineWebPerfTest.bat in Commandline with absolute path of the testcase file (<TestCase>.tst) as argument.
- This will generate report file `<testcasename>_report.txt` under `<QEngine Home>/projects/<projectName>/webperflogs/`. And the type file `<Testcasename>.prop` will generated under `<QEngine Home>/projects/<projectName>/webperflogs/type/`.

**See Also**

*Creating New Monitor - QEngine Script Monitors*
Web Transaction Monitors

Web Transaction Monitor enables you to monitor the entire End - to - End Web Transactions starting from the URLs to SQLs. Performance metrics of WEB components, EJB, Java and SQL statements executed by the URL can be monitored. Further, to identify bottlenecks in performance, individual methods of the various J2EE and Java components can be tracked.

Web Transaction Monitor requires an agent to be plugged in the server to be monitored. Know more about Web Transaction Agent.

Through the agent, the performance metrics data is collected for the URLs invoked by the server and is displayed in the web transaction monitor. Know more about Performance Metrics

See Also
Creating New Monitor - Web Transactions Monitor
Web Transaction Agent

Web Transaction Monitor requires an agent to be plugged in the application server (like JBoss, Tomcat) to be monitored. Follow the steps given below to deploy the agent:

- Copy the AdventNetWTA.jar present under <ApplicationsManagerHome>/working/classes to a local directory in the Application server (like JBoss, Tomcat).
- Edit the startup script of the application server (like JBoss, Tomcat) and add the below command line option to the java runtime environment
  
  -javaagent:<Path to the AdventNetWTA.jar>

- Restart the Application server (like JBoss, Tomcat).
  
  For e.g., To enable Web Transaction Monitor in JBoss applications Server, do the following:

- Copy the web transactions agent(AdventNetWTA.jar) under <ApplicationsManagerHome>/working/classes to a local directory of the server where JBoss is installed.
- Edit the run.sh/bat under JBoss home/bin. Append the following command to JAVA_OPTS
  
  JAVA_OPTS =-javaagent:<Path to the AdventNetWTA.jar>

- Restart JBoss.

Web Transaction Agent Port:

The default port of the agent is 55555. But, if you want to change the default port, Add -Dam.wtaconf.dir =<directory in which the wta.props file is present> in JAVA_OPTS

Next, you should add port=<port no> in wta.props file.

To verify if the agent has started, look for the message 'AdventNet Web Transaction agent started at port <55555>' in the startup logs.

By default, only the standard J2EE classes are instrumented for performance metrics. This includes Servlet, JSP, EJB and JDBC classes. In order to collect metrics for the user's Java classes the <wta.props> file needs to be configured. This file should be placed in the <conf> directory.

The following entries have to be edited in the file

- package-list : This is a comma separated list of the packages that have to be selected for instrumentation. (The package names can be truncated, for e.g., <com.test.server.accounts> can be specified as <com.test.server>.
- package-rule: This can contain a value of "include" or "exclude". If specified as include then, only the packages present in the package-list are selected for instrumentation. If specied as exclude then all the packages except for the ones mentioned in the package-list are selected for instrumentation.

Note: This file should be used judiciously because unwanted packages selected for instrumentation will create additional performance overhead on the system.

See Also

Creating New Monitor - Web Transactions Monitor
Web Transaction Metrics

The execution time of the URL and status is displayed along with the performance data for the various components like WEB, EJB, Java and SQL. By clicking on a specific URL, the execution details (Trace) for that particular URL is displayed as a tree structure. The trace will chart the sequence of the internal invocations (methods) of the URL.

In the trace, details of the Methods, like Type of method (Servlet, JSP, JDBC, etc,) Status of the method (GOOD / ERROR), Execution time is shown. If an SQL is invoked, the SQL Query that was executed would be displayed under More Info. Clicking on Tree will give you the entire list. Clicking on the respective components like WEB will list the various methods of that component alone.

Alert Configuration:

By clicking on the Configure Alert icon, you would be able to configure alerts based on the following attributes

- TotalExecution Time
- WebExecution Time
- JavaExecution Time
- JDBCExecution Time
- EJBExecution Time

You can then associate Thresholds like Response Time and actions like Send Email for the individual URLs, which will be escalated if response time of that particular URL is critical. Know more on alert configuration. Action can be configured at the monitor level for the Health and Availability. The alerts for a particular URL will be escalated to the monitor.

Note: To update the monitor with current data, click Refresh Data link.

Edit Monitor:

By clicking on the Edit Monitor icon, you would be able to edit the configuration details of the monitor.

- Enter the Display Name of the monitor.
- Enter the desired Polling Interval. By default it is 10 minutes.
- Data collection in the Web Transaction Agent can be turned off entirely, by deselecting this option.
- Enter the Sampling Factor. This attribute controls the data collected in the agent. It is the total execution count of an URL after which the statistics is collected. For eg., if the sampling factor is configured as 100 then data will be collected for one in every 100 execution of an URL.
- To control the web transaction agent memory
  - You can choose the maximum number of URLs whose details are stored in the agent at any given point of time. It would be the set of URLs who have the worst performance i.e., maximum execution time
  - Option is given to include or exclude specific packages to be monitored. The agent has to be restarted for the changes to take effect.
  - You can choose to enable or disable trace. If you disable trace then, only data of the top level transaction is collected.
    - You can choose the maximum depth of methods that need to be stored in the Agent.
      For eg., AccountServlet
      AccountEJB
      ...
      Statement.execute
You can choose the **maximum number of children** methods that need to be stored in the Agent.
For eg.,
AccountServlet
AccountSQL
.
.
.
Account.JSP

- These parameters are used to control the amount of trace that would be stored and thereby boost the performance of the agent.

**See Also**
Creating New Monitor - Web Transactions Monitor
Configuring Alerts

What is an Alert?

Alert are notifications generated based on some condition or criteria, helping to detect problems when any of the servers running in the network is experiencing it. This improves the fault management ensuring productive application monitoring.

There are three severity levels for the alerts and they are

- Critical
- Warning
- Clear

Alerts are generated for the following type of attributes:

1. **Availability** of a Monitor. When the availability of the Monitor is down, the severity is represented as and when it is up, the severity is represented as.
2. **Health** of a Monitor.
3. **Attributes** of a Monitor. Alerts will be generated, if the threshold profile condition set for these attributes is met.

**Note:**

- The availability of a Monitor requires no configurations from your side.
- Alerts are also generated based on dependencies configured to the attributes. Refer to Configuring Dependencies section for more details.

The Alerts screen provides a Alerts Graph, Alert Views, Alerts list, and Quick Links.

- **Alerts Graph:** This graphically represents the number of alerts based on its severity.
- **Alert Views:** This is an option to view the alerts based on a particular Monitor Group or Monitor Type by selecting them from the respective combo box.
- **Alerts list:** This lists all the alerts with details such as Monitor name, Status, Alert Message, Date/Time, and Technician who attended on the alert. You have an option to display 25/50/75/100/125 alerts per page. Alerts can be acknowledged by the Technicians (Users) by picking up alerts, likewise unpicking of alerts is also possible. Options to add, delete and edit annotations is available. By Clicking on ‘Set as Clear’ link, you can change the state of the selected alerts from Critical/Warning to Clear state.
- **Quick Links:** Refer to the Alert Details section of Appendix.

The following steps will generate alerts and perform actions based on your configuration. Go through the following sections to know about the configurations.

1. Creating Threshold Profile
2. Creating Actions
3. Associating Threshold and Action with Attributes
4. Configuring Dependencies
5. Configuring Retry Polls

**Note:** Bulk Alerts Configuration is also possible. Refer Bulk Alert Configuration
Viewing and Configuring Alerts Globally

Configuring Alerts is the final step in monitoring your applications or services.

Once the Monitor is associated with the Monitor Group, alerts can be configured through the Configure Alert screen. This provides an overview of all the attributes of the Monitor in a Monitor Group, and the thresholds and actions associated with the attribute.

The purpose of Global Alert Configuration is that you can associate thresholds and actions directly rather than from the individual Monitor screen. Additionally, you can view all the thresholds and actions associated with the attributes of a Monitor Group / Monitor in a single screen.

You can perform the following functions in the screen:

- You can create and associate a threshold for an attribute by clicking ‘associate’ link. It opens the ‘configure alerts’ page, herein you can create a new threshold or apply an existing threshold for the attribute.

  Note: By selecting ‘Apply to all monitors’, the threshold for this attribute is applied to all monitors of the same type. For eg., say you are associating a threshold for Response time of a particular Linux server. By selecting ‘Apply to all monitors’, the threshold for response time is applied to all Linux servers.

  For more information, refer to the Associating Threshold and Action with Attributes section.

- You can edit already existing thresholds by clicking on the threshold name.

  Note: You can also view the Global Alert Configuration screen by clicking ‘Configure Alerts’ under admin tab.
Creating Threshold Profile

Thresholds let you define the status of an attribute based on specific conditions. For example, you can define a threshold to show the status of the web server as critical, if the response time exceeds 100 seconds. Likewise, you can define a threshold to show the status as clear, if the MBean's attribute - Active is equal to true.

To define a threshold, follow the steps given below:

1. Click New Threshold. This opens the Create New Threshold Profile screen.
2. Create New Threshold Profile for Numeric Values or for String Values
3. Specify the Threshold Name.
4. Specify the conditions for the different severity of the alerts. You can also specify a message that has to be appended to the alert. By default, you can configure Critical severity, By clicking on advanced, you can configure Warning and Clear severity.
5. Specify the number of polls that can be scheduled before reporting an error. By default, it takes the value from Global Settings. Refer Configuring Retry Polls for setting configurations for individual monitors.
6. Click Create Threshold Profile to add the threshold after defining all the conditions.
7. Choose the View Threshold option available in the top menu to view the threshold. The Threshold Profile screen lists all the default thresholds and newly created thresholds. Note: You can also edit the threshold created using the edit icon.

The thresholds thus defined can be associated with the attributes for determining the status of the attributes of the Monitor Group. You can also associate thresholds and actions directly through Global Alert Configuration instead of the individual Monitor screen.

Refer to Associating Threshold and Action with Attributes for more details.
Creating Actions

Applications Manager provides the flexibility in fault management by triggering actions, such as sending e-mail, SMS, trap, and executing a command, to notify you of the alerts generated while monitoring the applications. These corrective actions make fault detection easier and faster enhancing Monitor Group management.

To trigger such corrective actions, you should have defined the action, which can then be associated with an attribute. Applications manager supports the following actions:

- Send E-mail
- Send SMS
- Execute Program
- Execute MBean Operation
- Send Trap
- Log a Ticket
Sending E-mail

This action will send e-mail to the specified persons in the event of an alert. To create an e-mail action, follow the steps given below:

1. Click the New Action link at the top menu. It opens Send Email screen, by default. **Note:** If the mail server is not configured already, you will the Configure Mail Server screen initially. Specify mail server details and continue to configure Send E-mail action.

2. Specify the following details:
   1. Any **display name** for the action.
   2. The **from** and **to** e-mail addresses.
   3. The **subject** and **message** of the e-mail.
   4. Choose the format of the message: **HTML, Plain Text or Both.**
   5. Choose whether to append the alert information generated by Applications Manager to the Email.

3. Click **Create Action** to finish. This will list the e-mail action name and its details along with the other actions configured.

4. Click **Add New** for creating more e-mail actions or **Delete** (on selecting the respective action’s check box) to delete the action.

After creating an e-mail action, you can edit or execute that action. These two tasks can be performed from the “View Actions” page.

- To edit the action, click the **Edit** icon.
- You can also have a trial execution of the action. To do so, click the **Execute** icon of that action.

**Note:** The Subject and Message of the e-mail action can be further enhanced by using **Replaceable Tags.**
Sending SMS

This action can be used to send SMS (Short Message Service) to specific users in the event of the alert. To create an SMS action, follow the steps given below:

1. Select the New Action link from the top menu.
2. Click Send SMS from the Actions menu in the left frame and specify the following details:
   1. Any display name for the action.
   2. The from and to addresses.
   3. The message for the SMS.
3. Click Create Action to finish. This will list the SMS action name and its details along with the other actions configured.
4. Click Add New for creating more SMS actions or Delete (on selecting the respective action's check box) to delete the action.

Also refer "Add complete Information to SMS" section under Admin > Action-Alert-Settings.

After creating an SMS action, you can edit or execute that action. These two tasks can be performed from the "View Actions" page.

- To edit the action, click the Edit icon.
- You can also have a trial execution of the action. To do so, click the Execute icon of that action.

Note: The Message of the SMS action can be further enhanced by using Replaceable Tags.
Executing Program

On the occurrence of an alert, a specific program can be executed. To execute a program, follow these steps:

1. Select the **New Action** link from the top menu.
2. Click **Execute Program** from the **Actions** in the left frame and specify the following details:
   1. Enter the display name for the action.
   2. Enter the Program to be executed. Use the **Upload Files/Binaries** option to upload the script file .
   3. Enter the directory path from which the script should be executed.
   4. The **Abort after** field is used to specify the timeout value for the program. Specify the time after which the program should be terminated.

   **Note:** It is important to provide the required time for aborting the command execution since the alert processing is held up by the program execution. That is, while executing the program, the command runs synchronously in the mail alert processing thread. This will delay all the alerts, following the alerts being processed, until the program execution is completed or terminated.

3. Click **Create Action** to finish. This will list the Execute Program action name and its details along with the other actions configured.
4. Click **Add New** for creating more actions or **Delete** (on selecting the respective action's check box) to delete the action.

After creating an execute program action, you can edit or execute that action. These two tasks can be performed from the "View Actions" page.

- To edit the action, click the **Edit** icon .
- You can also have a trial execution of the action. To do so, click the **Execute** icon of that action.

**Note:** Passing arguments to custom scripts can be further enhanced by using **Replaceable Tags**.
Sending Trap

There are some circumstances where some Manager Applications also need to be intimated about occurrence of fault in the servers or applications being monitored. In such case, the alerts can be sent as traps to the manager applications and they can be viewed by any standard SNMP Manager such as Trap Viewer, HP Openview, IBM Tivoli etc. The supported versions of SNMP Trap are SNMPv1 and SNMPv2c.

To configure an alert as a trap and send it as an action, follow these steps:

1. Select the **New Action** link from the top menu.
2. Click **Send Trap** under the **Actions** menu in the left frame. This opens the **Create Send Trap action** screen.
3. Select the SNMP trap version (v1/v2c) from the combo box.
4. Specify the following details:
   1. Any display name for the action.
   2. The destination or the manager application **host name** to which the trap has to be sent.
   3. The **port number**, where the manager host is running.

   The following are the details required to be filled for a trap PDU:

   4. The **OID (Object Identifier)** of the management object of a MIB.
   5. The **community** for the trap.
   6. The message, which will be sent as trap varbinds. The message can be enhanced by using Replaceable Tags.

   **Note:** Multiple Varbinds can be specified by having multiple ObjectIDs and their values as comma separated in "ObjectID" and "Message (Varbinds) " field respectively. For e.g., you can give ObjID1, ObjID2, ObjID3 in the ObjectID field to represent 3 Object IDs and correspondingly give ObjValue1, $RCAMESSAGE (the root cause message will be passed through the replaceable tag - $RCAMESSAGE), ObjValue3 etc., in the varbinds field to specify the values. ObjID1 and ObjValue1 will be passed as varbinds, same is the case with the other varbinds.

   7. Select the **Generic type** of trap PDU from the combo box. Specify the **Enterprise OID** for the trap You can also use the MIB Browser to provide the OID. In case, you want to upload a new MIB, then use the Upload Files/Binaries option. In case of SNMPv2c trap, mention the **SNMP Trap OID**.

5. Click **Create Action** to complete the configurations. This will list the trap action name and its details along with the other actions configured.

6. Click **Add New** for creating more trap actions or **Delete** (on selecting the respective action’s check box) to delete the action.

After creating an send trap action, you can edit or execute that action. These two tasks can be performed from the “View Actions” page.

- To edit the action, click the **Edit** icon 📝.
- You can also have a trial execution of the action. To do so, click the **Execute** icon ⏯️ of that action.
Execute MBean Operation

Actions of type Execute MBean Operation can be created to invoke operations on MBeans of JMX Compliant Resources. The JMX compliant resources that are supported by Applications Manager are: WebLogic, WebSphere, JBoss, AdventNet RMI Adapter and JMX agents (JDK1.5 / MX4J). Creating a MBean Operation would be helpful if you want to monitor the value of any custom attribute and do any action based on its value.

For Eg. When you want to shut down your JBoss server when the number of threads running in it goes above a specified value, you can add the necessary code to shutdown the server on the JBoss Monitor side as a MBean operation and invoke this as a MBean Operation action from the Applications Manager.

To configure an Execute MBean, follow these steps:
1. Select the New Action link from the top menu.
2. Click Execute MBean under the Actions menu in the left frame. This opens the Create New MBean Operation Action screen.
3. By following a simple set of 4 steps you can create a MBean Operation. First Step : If you have a JMX compliant monitor already configured, it will be listed in the Combo box. Provide a name for the action and select any one of the resources for which you create a MBean Operation. If you donot have any monitor configured, use the link given the page to discover a new monitor. Click on the Show Domains Button to go to the next step.
4. Secondly, The list of domains present in the agent you have selected are displayed. Select any of the Domains and click on the button Show MBeans.
5. In the third Step, Select any one of the MBeans for which you want to create the action and click Show Operations.
6. All the MBean Operations are listed in this screen with varying return types and arguments. Click Create Action button for the operation for which you want to create this action. A success message that you have created this action would be displayed and the newly created action will be listed under the head Execute MBean Operations Action(s)

Note: You can give multiple values to the operation arguments as comma separated values. For an operation with multiple arguments, the combinations of the values supplied, can also be executed. This is done in order to ensure that we need not create separate actions to represent different combinations of argument values.

For Example, if you want to create actions for the logging level of a product, the operation change loggingLevel may take two arguments as, "User" and "Level". You can supply, admin and operator as values for User and debug and info for Level respectively. You can execute the operation manually by choosing any of the combinations using the "Manual Execution" option. By default the first values given will be taken to execute the action, as Admin and debug in the above example.

Passing multiple values can be further enhanced by using Replaceable Tags.

After creating an MBean Operation action, you can test the execution of that action in two ways:
- You can have a trial execution of the action. To do so, click the Execute icon of that action.
- You can also manually execute the action, click on this. This opens a popup with the operation details. Select the options from the list and click Execute Action button. The action would be called with the given values and return value will be given in the UI.
**Note:** There is a link **Fetch data now** in the corresponding monitor details page, which will fetch the data from the server, after you have executed the action. This will help you to see the value of the custom attribute without waiting for the next polling interval.
Log a Ticket

ServiceDesk Plus is a web-based Help Desk and Asset Management software, offered by AdventNet.

This action will send a Trouble Ticket to ServiceDesk Plus, in the event of an alert. To create a Ticket action, follow the steps given below:

1. Select the New Action link from the top menu.
2. Click Log a Ticket under the Actions menu in the left frame. This opens the Configure Ticket Details screen.
3. Enter the name of the Ticket.
4. Choose the Category, Priority and Technician to whom the ticket should be assigned, these ticket details will be tagged with the generated tickets.
5. Enter the title of the ticket, the title supports the usage of replaceable tags. You can add alarm variables to the title, by selecting those from the combo box.
6. Give the description of the mail content. The description also supports passing alarm variables as replaceable tags.
7. Choose the format of the message: HTML, Plain Text or Both.
8. You can choose whether to append the alert message that was generated, to the trouble ticket.

Note: More information on how to integrate ServiceDesk Plus with Applications Manager is available here.
Replaceable Tags

Alert Configuration can be further enhanced by 'Replaceable Tags'. An email action is configured, if, for e.g., Tomcat Server goes down. While creating the E-Mail action, you can specify the "Message" as say "This resource is running $HOSTNAME at port $PORT". If the Tomcat Server goes down, then email action is triggered with a message that contains the actual name of the Host and Port Number. Hereby the Dollar Tags are replaced with the host in which the tomcat server is running and the exact port of the tomcat server.

Further, if you want Applications Manager to pass arguments to Custom Scripts, which would be invoked as part of 'Execute Program Action', you can make use of Replaceable Tags. For e.g., in 'Execute Program Action', you can give the value for 'Program To Execute' to be 
<run.bat $HOSTIP $MONITORNAME $PORT>
If the action is invoked then the $tags would be replaced with the then actual values say
<run.bat 191.167.111.27 MyServer 9090>

Find below the dollar tag parameters that can be associated with their probable values.

<table>
<thead>
<tr>
<th>Tags</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$MONITORNAME</td>
<td>Name of the Monitor</td>
</tr>
<tr>
<td>$ATTRIBUTE</td>
<td>Various Attributes like Health, Availability, etc.,</td>
</tr>
<tr>
<td>$SEVERITYASNUMBER</td>
<td>1 (Critical/Down) 4 (Warning) 5 (Clear/Up)</td>
</tr>
<tr>
<td>$SEVERITY</td>
<td>Critical, Warning, Clear, Up and Down</td>
</tr>
<tr>
<td>$HOSTIP</td>
<td>The IP Address of the Host</td>
</tr>
<tr>
<td>$MONITORTYPE</td>
<td>Various Monitor Types like Tomcat-server, MYSQL-DB-server, Script Monitor, etc.,</td>
</tr>
<tr>
<td>$OBJECTNAME</td>
<td>MBean Object name when associated to Custom Monitor attributes</td>
</tr>
<tr>
<td>$HOSTNAME</td>
<td>Name of the Host</td>
</tr>
<tr>
<td>$PORT</td>
<td>Port Number</td>
</tr>
<tr>
<td>$RCAMESSAGE</td>
<td>Root Cause Message like Average Response Time of SQS_Tomcat-server_9095 is critical because its value 652 &gt; 10ms. [Threshold Details : Critical if value &gt; 10, Warning if value = 10, Clear if value &lt; 10]</td>
</tr>
</tbody>
</table>
Associating Threshold and Action with Attributes

The next step after creating the thresholds and actions is to associate them with the appropriate attributes of Monitor for generation of alerts. Follow the steps given below to associate a threshold and actions with an attribute:

1. Select the **Home** tab from the client.
2. Click the Monitor Group. This lists the Monitors in it.
3. Click the Monitor to whose attributes, threshold and actions must be associated.
4. Click **Configure Alert** from the respective attributes. The attribute name is listed in the combo box. You can either associate threshold or action or both.
5. To associate threshold, select the threshold from the **Associate Threshold** combo box. Click **View Thresholds** to view details about the selected Threshold. If no threshold is configured, select **New Threshold**.

   **Note:** By selecting 'Apply to all monitors', the threshold for this attribute is applied to all monitors of the same type. For e.g., say you are associating a threshold for Response time of a particular Linux server. By selecting 'Apply to all monitors', the threshold for response time is applied to all linux servers.

6. To associate action, select the action you want to perform from the Available actions and move it to the Associated Actions list box for each severity. Click **View Actions** to view details about the selected action. If no action is configured, click **New Action**.

7. Click **Save All** to save the configurations.

You can also associate threshold and actions from **Global Alert Configuration** screen.

The threshold and/or actions are now associated with the attribute. Based on this, alert will be generated and action will be performed for that attribute.

**Note:** Thresholds are configured and associated to attributes. You cannot associate threshold with attributes such as **Availability** and **Health**. Also in case of health, you must configure dependencies to generate alerts.

### Remove Configurations

You also have an option to delete/remove the above configurations using the **Remove Configurations** option. This will remove all the configurations and alerts.
Bulk Alerts Configuration

After configuring alert for a particular monitor, if the same configuration holds good for all other monitors of the same type, then by using Alert Template functionality you can do Bulk Alerts Configuration. Currently, Threshold and Action configurations are supported. It is very useful in cases where you want to configure identical Thresholds/Actions for a huge number of similar monitors.

For e.g., if there are ten Tomcat servers and you want to configure an email action, if the response time for Tomcat exceeds 100 seconds. The alert (Threshold and Action) is configured for one Tomcat server and by using Alert Template this configuration can be applied to all the other Tomcat servers.

Usage of Alert Template is illustrated below:

1. Click on the Alert Template link under 'Snapshot' of the particular monitor.
2. A popup opens up with two choices: Overwrite existing Threshold Configuration and Overwrite existing Action Configuration
3. If you choose to overwrite the existing Threshold Configuration, then Thresholds already associated would be overwritten with the new configuration, otherwise the old setting is retained.
4. If you choose to Overwrite existing Action Configuration, then actions already associated, are removed and the new configuration added. Otherwise new configuration is appended to the existing configuration.
5. On clicking on Apply, the alert configuration is applied across all monitors of the same Monitor Type.
Configuring Dependencies

Dependencies determine the health/availability of a Monitor Group or Monitors. They consist of the dependent parameters of the Monitor based on which the severity of the health and availability are determined.

By configuring dependencies, you can specify whether the health or availability depends on all or few dependencies. The severity is also determined by order of severity which is given below:

1. Critical
2. Warning
3. Clear

For example, If there are 9 dependencies in a Monitor Group where three are critical, three are warning, and three are clear and the severity of Health of Monitor Group is based on any three selected dependencies, then the severity will be Critical as per the order of severity.

Configuring Dependencies

To configure dependencies for the Monitor or Monitor Group, do the following steps:

1. Select the Home tab that lists all the Monitor Groups.
2. Click on the Monitor Group that lists the Monitor.
3. Click on the Configure Alert icon of the respective Monitor. This opens the Configure Alert screen.
4. Choose Health or Availability from the combo box. The dependent attributes will be shown in the list box under dependencies.
5. Select and move the required attributes from the left box to the right box using >> button. By default, all the dependencies for the attributes of the monitors are added in the right box. You can also remove the default settings using the Action / Alert Settings option.
6. Specify whether the rule for determining the severity for health or availability.
   
   **Depends on all selected parameters:** The severity of health depends on the severity of all the selected parameters.
   
   **Depends on any "n" selected parameters:** The severity of health depends on only 'n' selected parameters. The number of parameter, n has to be selected from the combo box.

7. Click Save All to complete configuring dependencies.
Configuring Retry Polls

If you do not want Applications Manager to generate alert for the first time the threshold condition is crossed, then you can use this option to specify the number of consecutive polls before generating an alert. For e.g., If you want an email alert to be generated only if the CPU Disk utilization is above 100%, consecutively for more than two polls, then you can configure the number of consecutive polls before reporting an error as two. In global settings, you can have a common setting for all the monitors. Refer to Action / Alert Settings for more information.

If you want to overwrite the common settings, you can also configure the polls before reporting an error on availability and threshold of individual monitors.

To Configure Retry Polls on Availability for Individual monitors

1. Click on Configure Alert icon, in the 'Today’s availability' graph of the selected monitor.
2. You can configure the number of times consecutive polling should take place before reporting that the monitor is up or down.
3. You can also click on the Configure Alert Link in the Snapshot view of the monitor, and by clicking on the Configure Alert icon, for availability attribute, you can configure the retries.
4. You can enter the number of times consecutive polling needs be done before reporting that the availability is up or down. You can leave the 'Polls before reporting an error' field empty to have the global settings for retries take effect.

To Configure Retry Polls on Threshold for Individual monitors

1. Click New Threshold Profile. This opens the Create new Threshold Profile screen.
2. Create New Threshold Profile, as per details found in Creating Threshold Profile.
3. Note: Specify the number of polls that can be scheduled before reporting an error. By default, it takes the value from Global Settings. For e.g., if you have created a threshold for web server to be critical if the response time crosses 100 seconds. And you wish to receive an email alert only if the web server becomes critical after two polls and not at the first poll itself. Then configure the number of polls before reporting an error as two. You can leave the 'Polls before reporting an error' field empty to have the global settings for retries to take effect.
Viewing Reports

An important aspect of all management tasks is that you can analyze the trend over time and evaluate the performance. The analysis is also useful in making calculated predictions and taking corrective actions as necessary.

Applications Manager generates reports that help you to analyze the performance of your Monitor Group. The reporting function enables you to analyze your servers / applications / services even across months and all this even without having to make any additional configuration changes.

To view the reports, you can follow either of the given steps:

- Click the **Reports** module tab. This opens the index page that lists all the reports generated by Applications Manager (or)
- Click on the Monitor Group and select **Application Report** Link in the left frame. By default, it takes you to the **Availability** report of the Monitor Group.

The report depicts the availability, health, response time and alerts of the application over a specified period of time. Some **additional features** in Report Generation are:

- Options to view 10/20/50/All reports by choosing them from the **Top N Reports** field. By default, it shows top 10 reports.

**Note:** This is not applicable to reports generated for Monitor Groups.

- Option to view the following reports for all individual monitors
  - Downtime History Reports: Gives the downtime/uptime chart for 'today''s period and also the downtime history for that particular monitor across all time periods.
  - Summary Reports: Gives the summary of all the reports for that particular monitor.

- The Reports page contains a list of reports generated using Applications Manager by grouping them with respect to Monitor Groups and Monitor Type. To know more details, refer to the **Grouping of Reports** section.
- Option to view report on last seven days data by clicking on **7** Icon. It also opens up to a page where we can get thirty days data by clicking on **30** Icon
- Option to view Custom Time Period reports for Availability and Attributes, i.e, the time period for which the reports are needed can be selected.
- Option to save the reports in CSV format by clicking on **CSV** icon and also PDF format by clicking on **PDF** icon for each individual report under reports tab.
- Option to delete known downtime reports.

**Note:** Scheduling of reports is possible by using **Schedule Reports** under Admin tab.
Grouping of Reports

The Reports page contains a list of reports, generated using Applications Manager, by grouping them with respect to Monitor Groups and Monitor Type. The reports are grouped for easier report analysis and for providing more flexibility in report generation. They are grouped as follows:

- Monitor Group
- Individual Monitors
- Application Servers
- Database Servers
- Services Reports
- Mail Server Reports
- Server Reports
- Web Services Reports
- Custom Monitor Reports

Note: The details available for each attribute of the Monitor Type (except Monitor Groups) are shown in descending order. For example, in Availability report of a Monitor Type, the Monitor with the poorest availability is displayed first.

Monitor Group Reports

This generates reports for all the Monitor Groups created using Applications Manager. Choose the Monitor Group from the Select Application combo box. The following are the different Report types that are generated for the Monitor Group.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of all Monitors</td>
<td>The overall availability of all the monitors, and the availability details for the respective monitors in the Monitor Group.</td>
</tr>
<tr>
<td>Monitors by Health</td>
<td>The overall health of all the monitors, and the health details for the respective monitors in the Monitor Group.</td>
</tr>
<tr>
<td>Monitors by Response Time</td>
<td>The minimum, maximum, and average response time of all the monitors being monitored by the Monitor Group, in milliseconds.</td>
</tr>
<tr>
<td>Monitors by Alerts</td>
<td>Alert Occurrences for the application, attributes grouped in the application, and monitors, with graphical representation. Additionally, a graph representing the split up of total critical alert occurrences in application by most critical monitors is also generated.</td>
</tr>
</tbody>
</table>

Individual Monitor Reports

This generates reports for the individual monitors. The following are the different Report types that are generated.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime History</td>
<td>Gives the downtime/uptime chart for &quot;today&quot;s period and also the downtime history for that particular monitor across all time periods.</td>
</tr>
<tr>
<td>Summary Report</td>
<td>Gives the summary of all the reports for that particular monitor.</td>
</tr>
</tbody>
</table>
Application Servers Reports

This generates reports for the Application Server Monitor Type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing **ALL** from the combo box) or for any specific Monitor Type (by choosing the respective type of Application Server Monitor Type from the combo box). The following are the different Report types that are generated for the Application Server.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Application server Monitors being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager server.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The minimum, maximum, and average response time of all the Application server monitors, in milliseconds.</td>
</tr>
<tr>
<td>JVM</td>
<td>The minimum, maximum, and average JVM usage by all the Application server monitors, in bytes.</td>
</tr>
<tr>
<td>JDBC Connection Usage</td>
<td>The minimum, maximum, and average JDBC Connections of Application server monitors</td>
</tr>
<tr>
<td>Thread</td>
<td>The minimum, maximum, and average number of threads spawned by Application server monitors</td>
</tr>
<tr>
<td>HTTP Session</td>
<td>The minimum, maximum, and average HTTP Sessions of Application server monitors</td>
</tr>
</tbody>
</table>

Database Reports

This generates reports for the Database Monitor Type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing **ALL** from the combo box) or for any specific Monitor Type (by choosing the respective type of Database Monitor Type from the combo box). The following are the different Report types that are generated for the Database monitor.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Database Monitors being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager server.</td>
</tr>
<tr>
<td>Connection Time</td>
<td>The minimum, maximum, and average time taken to connect to the database server by the Applications Manager server, in milliseconds.</td>
</tr>
<tr>
<td>Buffer Hit Ratio</td>
<td>The minimum, maximum, and average Buffer Hit Ratio of the database</td>
</tr>
<tr>
<td>Cache Hit Ratio</td>
<td>The minimum, maximum, and average Cache Hit Ratio of the database</td>
</tr>
</tbody>
</table>

Service Reports

This generates reports for the Service Monitor Type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing **ALL** from the combo box) or for any
specific Monitor Type (by choosing the respective type of Service Monitor Type from the combo box). The following are the different Report types that are generated for the Service Monitor Type.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Service Monitors being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager server.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The minimum, maximum, and average response time of all the Service monitors, in milliseconds.</td>
</tr>
</tbody>
</table>

**Mail Server Reports**

This generates reports for the Mail Server monitor type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing ALL from the combo box) or for any specific Monitor Type (by choosing the respective type of Mail Server Monitor Type from the combo box). The following are the different Report types that are generated for the Mail Server Monitor Type.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Mail Server Monitors being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager Mail Server Group.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The minimum, maximum, and average response time of all the Mail Server monitors, in milliseconds.</td>
</tr>
</tbody>
</table>

**Server Reports**

This generates reports for the Server Monitor Type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing ALL from the combo box) or for any specific Monitor Type (by choosing the respective type of Server Monitor Type from the combo box). The following are the different Report types that are generated for the Server Monitor Type.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Server Monitor Types such as Linux and Windows being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager server.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The minimum, maximum, and average response time of all the Server Monitors, in milliseconds.</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>The minimum, maximum, and average amount of CPU utilized by the Server Monitor.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>The minimum, maximum, and average amount of memory utilized by the Server Monitor.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>The minimum, maximum, and average amount of Disk space utilized by the Server Monitor.</td>
</tr>
</tbody>
</table>
Web Service Reports

This generates reports for the Web Service Monitor Type created using Applications Manager. The reports can be generated either for all the Monitor Types (by choosing ALL from the combo box) or for any specific Monitor Type (by choosing the respective type of Web Service Monitor Type from the combo box). The following are the different Report types that are generated for the Web Service Monitor Type.

<table>
<thead>
<tr>
<th>Report Types</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The availability details that include total down time in hours and minutes, average time taken to repair the failure (MTTR), average time between the failures (MTBF), and average Uptime percentage for all the Web Service Monitors being monitored by the Applications Manager.</td>
</tr>
<tr>
<td>Health</td>
<td>The health of all the monitors in the Applications Manager server.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The minimum, maximum, and average response time of all the Web Service monitors, in milliseconds.</td>
</tr>
</tbody>
</table>

Custom Monitor Reports

This generates report for all the numerical attributes of the Custom Monitors created using Applications Manager. The list of all the scalar numerical attributes available in the Custom Monitor will be listed with the reports and the agent name.

The following are the parameters in the report details of any attribute for which the report generation is enabled.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
</table>
| Attribute Details | This contains the following details:  
  • Name of the attribute.  
  • The agent from which the attributes were added to the Custom Monitor.  
  • The port at which the agent is running.  
  • The type of the service or resource through which the JMX or SNMP agents are monitored.  
  • The minimum value obtained for every polling interval.  
  • The maximum value obtained for every polling interval.  
  • The average value of the attribute obtained for every polling interval. |
| Average Value | Graphical representation that depicts the relationship between the average value and time of the attribute. |
| Time         | Tabular representation that shows the relationship between the average value and time of the attribute. |

If the custom monitor is created and the attributes are not listed, then you can click on the link provided in the Custom Monitor Reports to enable or disable the same.
Performing Admin Activities

Applications Manager enhances effective business management allowing the system operators and administrators to configure any activity with ease.

The Admin module tab in the client lists all the administrative functions that can be performed with the product. The following are group of activities performed by the system administrators to monitor their system/service/application running in the network through Applications Manager. Click on the respective topics to know the details.

Monitors
- New Monitor Group
- New Monitor
- Thresholds
- Actions
- Configure Alerts
- Action / Alert Settings
- Availability Settings
- Network Discovery
- Bulk Configuration of Monitors
- Performance Polling
- Event Log Rules

Applications Manager Server Settings:
- Global Settings
- Configure Mail Server
- Configure Proxy
- Upload Files/Binaries
- User Administration
- Personalize Web Client
- Add - on Products Settings
- Product License
- Database Retention
- Google Map

Tools:
- Downtime Scheduler
- SNMP Trap Listener
- Schedule Reports
- Manager Console
**Action / Alert Settings**

This section explains the Action / Alert Settings that can be made in Applications Manager. To access Action / Alert Settings, click the **Admin** tab and click **Action / Alert Settings**.

**Enable Actions**

When alerts are generated, actions are triggered for those alerts (if you have configured any). If you do not want the actions to be executed in spite of the alerts, deselect this option.

**Add complete Information to SMS**

By default, the complete information that you configure while adding SMS Action is sent through the SMS. Some SMS service providers restrict the length of characters sent through the SMS. This could result in truncated message delivery. If you would want to send only information on the Monitor, Attribute, and its Severity, deselect this option. For E.g., "Health of JBoss Server is critical" will be the SMS format that is received.

This is in addition to the message provided when creating the SMS action.

**Execute Actions Repeatedly**

If you want the actions to be trigged continuously during every poll, till alerts change from Critical/Warning to Clear, you can use this functionality. The three types of recursive actions that are involved are

- If a Monitor is down, you can execute actions repeatedly till the Monitor is up.
- If Health is critical/warning, you can execute actions repeatedly till the Health is clear.
- If the attribute status is critical/warning, you can execute actions repeatedly till the attribute status is clear.

**Add Monitor’s attributes as dependencies, for Root Cause Analysis (RCA)**

By default, all the attributes of a monitor are added as dependencies to the health attribute of the monitor. If you do not require the attributes to be added, deselect this option. You can also manually add/remove dependencies later at any point of time.

**Polls before Reporting an Error**

The Critical, Warning, and Clear alerts are generated based on attributes that you have configured. You have control over the alerts that are being generated. Simply specify the number times after which the alert should actually be generated. It would eradicate false alarms.

If you want to poll ‘3’ times before reporting that a system (or any Monitor) is down or an attribute is critical, specify the value as ‘3’ in the first text box. Similarly, you can change the remaining two text boxes (warning, Clear) also. If you have set the poll as ‘2’ times before reporting a service is up, for the first time of polling, the service will be shown as Unknown. Only on the second poll, if the service is running, the status would be shown as ‘Up’. Changes made will be reflected across all the monitors.

Apart from Global settings, Polls before reporting an error, can be configured for threshold and availability of individual monitors. Refer Configuring Retry Polls.
Availability Settings

This section explains the availability settings that can be made in Applications Manager. To access availability Settings, click the Admin tab and click Availability Settings.

Show Monitor status as Up during Maintenance

Using Downtime Scheduler, you have the option to schedule a time period for which monitoring is not needed. If you want to show the availability of monitors under maintenance as Up, irrespective of their previous state, select this option.

Check for Network Availability

When the Applications Manager is out of the network or is not connected to the network, the status of all the Monitors that are currently been monitored will be shown as 'Down'. You can avoid this by enabling the 'Check for Network Availability' option.

When this option is enabled, Applications Manager will generate alerts for the unavailability of resources only if the specified host is reachable in the network. For example, let us assume that the system/host which runs the Applications Manager has been isolated from the network. Enable this option and specify a hostname in the network (preferably not the hostname where Applications Manager runs). Now, Applications Manager tries to ping that machine for its availability in the network. If not available, alerts are not generated and resources are not shown as down.

You can also specify the IP of your routers, gateways, etc., to check the system/host which runs the Applications Manager is present in the network.

Check for URL Availability

When the Applications Manager is out of the network or if external proxy settings are not configured, the status of all the URLs that are currently been monitored will be shown as 'Down'. You can avoid this by enabling the 'Check URL Availability' option.

When this option is enabled, Applications Manager will generate alerts for the unavailability of URL only if the other specified URL is down. For example, let us assume that the system/host which runs the Applications Manager has been isolated from the network. Enable this option and specify another URL which is expected to be up always. Now, Applications Manager tries to monitor URL for its availability. If not available, alerts are not generated and URL is not shown as down. Further a mail is sent to the configured mail address intimating the same.
Network Discovery

Network Discovery is the process of discovering all Monitors in a specified network. It discovers Monitor running in the default port only.

To discover all the Monitors in a network:

1. Click the Admin module tab.
2. Click Add under Network Discovery from the Admin Activities. This opens the Configure Network Discovery screen.
3. Enter the Network IP Address.
4. Enter the SubNetMask of the network.
5. Click Start Discovery to start discovering Monitor within the mentioned network.

| Note: To view the Monitors discovered in the network, click the Configured Networks link available in the left frame under Discovery Links or in the Admin module tab, under Network Discovery, click View. |

See Also

- New Monitor
- Network View
Bulk Configuration of Monitors

Selecting this option, would enable you to perform bulk administrative operations on Monitors. Clicking on this link, will take you to the Monitors bulk config View - where all monitors are listed.

You can perform the following Monitor Admin Operations:

Manage/Unmanage Monitors:

This option enables you to choose the monitors that you want to monitor or not. Under Monitors tab, select 'Bulk Config' view, here all the monitors discovered are listed. Select the monitors for which data collection needs to be done and then click on Manage link, likewise select the monitors for which you do not want data collection to happen and then click on Unmanage link. For license information, the count of the 'number of monitors' would be based on the number of Managed Monitors.

Update Username/Password:

This option enables you to bulk update usernames and passwords across monitor types.

For eg., if you have five tomcat servers running, you can select all the five tomcat servers from the list. Click on Update Username/Password. Your selection would be listed and you can enter the username and password that is common across all the five tomcat servers.

Copy and Paste Monitors:

This option enables you to copy and paste the configuration of one monitor to create new monitors of the same type. For eg., if you want to monitor the apaches running in 10 different servers, then you can configure the monitoring parameters of one apache in Host1 and copy those configurations to the other apaches in Host2, Host3 ..to..Host10.

On clicking copy and paste icon, you need to enter the host names of the servers to which the configurations have to be pasted (the host names can be given comma separated). Enter the SubNet mask too.

Note: If you want to copy and paste the configurations of server monitor, then you can choose to copy the configuration of the services running inside the server or only the server configuration.
Performance Polling

Using this option, Performance Data collection can be scheduled for the given number of polls. Except for Availability check and health, other performance parameters like memory usage data can be collected at the scheduled number of polls. This would be helpful in decreasing the load on the system of the users who want to monitor availability and health alone.

For eg., If the polling interval of a particular server monitor is one minute and the performance data is scheduled to be collected once in five pollings. In this case, the availability of the server is checked every minute whereas the performance data like CPU Memory is collected every five minutes.
Windows Event Log Rules

By using this option, you can monitor various windows events. The events received will be displayed in the Windows Monitor details page. Also, you can generate alerts in Applications Manager based on the configured rule. For eg., When an event of type Error occurs in System Log, you can generate a critical alert which inturn will affect the Health of the Windows Monitor.

Note: Event Log Monitoring is available in Windows Installations and also in WMI mode of monitoring only.

For receiving windows events, you have to configure Event Log Rules. You can get notified by the events from the following Log Files
- Application (By default Event Log rule is configured for any Application Error)
- System
- Security (By default Event Log rule is configured for any Security Failure)
- File Replication Service
- DNS Server
- Directory Service

Follow the steps given below, to add a new Event Log rule:
- Under Admin tab, click on **Event Log Rules**
- Click on ‘Add New Rule’
- Enter the **Rule Name** of your choice
- Enter the **Event ID** associated with the Event Log File (not mandatory)
- Choose the **Event Type** - Error, warning, Information. In case of Security Events, the types would vary between Success Audit and Failure Audit
- At the outset, you can enable or disable the Rule Status
- By clicking on **Advanced Options**, you can formulate the rule more specifically by associating the source, category, username, and description content of the incoming event to the alert severity.

For Eg., select Log File as [System] and Event Type as [Error] , to get all events of type Error from System Log File.
Global Settings

This section explains the global settings that can be made in Applications Manager. To access Global Settings, click the Admin tab and click Global Settings. On performing any of the configurations, click Update Global Settings button provided at the bottom of the page.

General

Show Help in Monitor Group Wizard

Applications Manager provides easy-to-use wizard when you click ‘New Monitor Group’ that explains how to create a new Monitor Group and Monitors. If you do not want to view the help content, deselect this option.

Show Intro Tab

When you login to the Web Client, you see an Intro page which helps novice users to understand the terms used in the product and to get started. If you want the Introduction page to be displayed, select this option.

Do not hide Advanced configuration in Alert Configuration

By selecting this option, you can always have all the advanced options expanded by default in the "Configure Alerts" and "New Threshold" screens.
By default, while configuring actions at attribute level, only the 'Critical Severity' actions can be associated with the Health of the attribute. Associations of Warning and Clear severity actions are hidden.
Likewise, by default, while creating new Thresholds, only the critical threshold is set. Warning and clear thresholds are hidden.
This is to aid customers who require only the critical configurations and they may not be interested in fine grained configuration of thresholds & alerts.

Add Host as a Monitor when you associate a service running in it to the monitor group

By default, when you associate a Monitor (service or server running in particular host) with a Monitor Group, the host (in which the Monitor runs) is also associated with the Monitor Group. If you do not require the host to be associated with the Monitor Group, deselect this option.

For example, if you are add and associate a monitor (say WebSphere) with a Monitor Group, Applications Manager will add and associate the host (say Windows) also in which the WebSphere runs with that Monitor Group.

Note: This host will be monitored only if you have provided the required configuration information.

Restart Applications Manager in case of serious server error

By selecting this option, you can restart Applications Manager automatically, incase any serious server error like out of memory error occurs.

Show inline feedback form

By selecting this option, you allow the inline feedback form in all pages.
Logging

By default, the debug prints are added to log files and are placed under `<Applications Manager Home>/logs` directory. You can configure the logging mechanism using the following **Logging Settings**.

- **Stop logging**: If this option is selected, debug prints are not added to the log files.
- **Print Fatal errors only**: If this option is selected, the debug prints are added to the log files only when there are fatal or critical errors in the functioning of Applications Manager.
- **Print Warning errors only**: If this option is selected, only the warning level debug prints are added to the log files.
- **Print all logs**: This is the default setting. All debug prints are added to the logs generated by Applications Manager.
Configure Mail Server

Mail servers are configured to send e-mails to desired destinations. For instance, when you perform an action to send e-mail for some alerts, you need to configure mail server through which mails are sent. Follow the given steps to configure mail server.

1. In the Admin page, click **Configure Mail Server**.
2. Provide the SMTP server name and the port number.
3. Provide the **user name** and **password**, if the SMTP server requires authentication details.
4. Click **Save** to save the configurations.

The SMTP server is configured and all the e-mails will be sent through this server.
Configure Proxy

In situations where any URL to be monitored is available in the Internet, then the requests have to be routed through a proxy server. Such URL monitoring can be performed by setting the proxy configuration. Follow the steps given below to configure a proxy server:

1. In Admin page, click **Configure Proxy**.
2. Select **Automatically detect settings**, if the proxy is to be detected automatically.
3. To specify the proxy settings manually, select **Use a proxy server** and specify the following details:
   1. Host and port number of the proxy server.
   2. User Name and password of the user to access the Internet.
   3. Specifies whether you want to use the proxy server for all local (intranet) addresses. Because a proxy server acts as a security barrier between your internal network (intranet) and the Internet, you could need extra permissions from your system administrator to gain access to Web pages through a proxy server. You might be able to gain access to local addresses easier and faster if you do not use the proxy server.
   4. Specify Internet addresses you want to connect to without using a proxy server. For example, you might not want to use the proxy server to contact other computers on your local network. Use semicolon (;) to specify multiple IPs.
4. Click **Save**.

All request to the Internet will then be routed through the proxy server.
Upload Files/Binaries

This is an option to upload the required files such as jars, zip, MIB, and scripts (batch and shell) into Applications Manager directory, without much of manual effort. You just have to provide the file by browsing it from your local machine and it gets automatically uploaded to the required directory of Applications Manager. Follow the given steps to upload a file.

**Note:** By default, the Upload Files/Binaries page is enabled in the Web Client. As an administrator, if you want to disable this option, follow the steps given below.

1. Edit the file `AMServer.properties` located in the `<Applications Manager Home>/conf` directory.
2. Set the value of `am.upload.enabled` as `false`.
3. Restart the Applications Manager server.

To enable this page, set the value of `am.upload.enabled` as `true`.

1. In Admin page, select **Upload Files/Binaries**.
2. Click **Browse** to locate the file to be uploaded in your local machine. **Note:** The file to be uploaded must be present in your local machine.
3. Choose the type of Upload such as JAR/ MIB/ Script. The purpose of choosing the type is to upload the files in the directories mentioned for each type of upload.
4. Click **Upload** to upload the files to the desired directory of Application Manager Home. You can also see the Application Manager Home directory below the File Upload table.

The uploaded files will be available under the specified directory of Application Manager and can be used for other operations.

The following files can be uploaded to the Applications Manager using the **Upload Files/Binaries** option.

- MIB file for Sending Trap Action
- Script file for Executing Program Action
- MIB file for adding SNMP OID attributes in Custom Monitors

The user can alternatively

- Put the MIBs in mibs folder eg : `<AppManager6-home>\working\mibs`.
- Scripts for execution in the `<AppManager6-home>\working` or `<AppManager6-home>\resources` folder and then give the path appropriately with respect to the `<AppManager6-home>\working` folder.
User Administration

Applications Manager permits three types of user access to work with the product. The different roles are:

- User
- Operator
- Administrator
- Manager

User

The system users have read only access to all components of the product. You will not have the privilege to access, configure or edit the different components of the product.

Operator

The system operators have read only access to those components of the product that the administrator assigns to the operator. You will not have the privilege to access, configure or edit the different components of the product. If operator is part of a Monitor Group, then the restrictions will take effect only for the operator and not others.

Administrator

The system administrators are allowed to perform all admin activities as explained in Performing Admin Activities. You also have the privilege to configure user administration as explained below.

Applications Manager allows the system administrators to configure any activity with ease. To create a new user access, follow the given steps:

1. In Admin page, click User Administration under Global Configurations. This lists the User Profile(s) that consists of the User name and the role.
2. To add a new user, click Add new. This opens the 'Configure User' screen.
3. Specify a unique User name and password. The description and e-mail info are optional.
4. Choose the role (User/Operator/Administrator).
5. Click Create User to complete the task.

**Note:** The default user access of Applications Manager is admin (Administrator). All users log into Applications Manager as Admin users and are given all the administrative privileges to work with the tool.

Manager

The Manager has an integrated high-level view of the Business Infrastructure. Service Level Agreements (SLAs) can be created and associated with various business applications and servers. More information on Manager role can be viewed here.

**Note:** You can assign the owners for the Monitor Groups while creating the Monitor Groups or while editing the existing Monitor Groups

To delete a user

1. In Admin page, click User Administration under Global Configurations.
2. Select the user(s) to be deleted.
3. Click Delete.
Personalize Web Client

This provides you an option to view the Application Manager client with a different look and feel as you prefer. You can choose the color of your preference from the colors listed in the Personalize Web Client screen. The available colors are:

- Blue
- Green
- Gray
- Brown
- Orange

Follow the given steps to personalize your Application Manager client's look and feel.

1. Select **Personalize Web Client**. A window that lists all the colors pops up.
2. Select the color of your choice by enabling the respective color. The default color is green.
3. Click **Apply**. This changes the color of the client's look and feel.
Add On - Products Settings

ManageEngine ServiceDesk Plus is a web-based Help Desk and Asset Management software, offered by AdventNet.

This section describes the method in which ServiceDesk Plus Settings are to be configured in Applications Manager.

- Under Admin Tab, click on ServiceDesk Settings
- Enter the **ServiceDesk Plus Server Details**
  - Enter the Name of the server where ServiceDesk Plus is running.
  - Enter the Port Number of that server.
- Enter the **Authentication Details** of the ServiceDesk Plus Server - Login and Password.
- Enter the **Email Address** configured in ServiceDesk Plus. All the trouble tickets generated would be sent to that Email ID.
- Enter the Email Address from which the trouble tickets should be sent.
- Test if the connection is working and save the settings.

To know more on how to integrate Applications Manager with ServiceDesk Plus, Click [here](#).

**Note:** By clicking on the Jump To link in the Web Client, You can shift to ManageEngine ServiceDesk Plus
Database Retention

To plot graphs and generate reports, Applications Manager collects data from the monitors at regular intervals. By default, Applications Manager 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. The aggregated data will be used in graphs and reports.

Applications Manager allows you to maintain the database with the required data. By default, the detailed data will be maintained for 5 days, the hourly data for 90 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 retention, follow the steps given below:

- Click on the Admin tab
- Under Global Configurations, click on Database Retention.
- Enter the number of days for which hourly statistics should be maintained.
- Enter the number of days for which daily statistics should be maintained.
- Enter the number of days for which alert statistics should be maintained.
- Then Save the changes.
Google Map Business View

The Google Maps API embed Google Maps in web pages with JavaScript. By integrating with Applications Manager, the status of all the monitor groups across the globe can be represented visually. The root cause analysis (RCA) data is available in the map.

To represent **Monitor Groups** in Google map, follow the given steps.

1. While creating a new monitor group, you can associate the monitor group to the location chosen from the list.
2. Else, click on **Add Location**, it opens up a google map. From the map, you can select and add custom locations.

**Steps to configure Google Map in Applications Manager web client**

1. Register for Google Map API Key in the following link
   http://www.google.com/apis/maps/
2. Give the Applications Manager client URL for eg., http://appmgrmachine:9090, while registering for the key.
3. Below is a sample key:
   <ABQIAAAACGngMDPPB5ol4nESiM6FSBSn6w5ihTF9sPvmIkeTzJnqPStjkhQTWehatYnC0-aTrxXpt9ddgdG_Nw>
4. In Applications Manager, under Admin tab, click on Google Map.
5. Enter the **Google Map key**.
6. You can add or delete location from the 'Manage Location' drop down box
7. You can then customize the Height and Width of the Google Map

**Note:** Get to know and verify the Google Map API Terms of Use
Downtime Scheduler

This provides you an option to schedule a time period for which monitoring is not needed. You can choose the time period recurrence as follows

- Daily
- Weekly
- Random

You can add a new Schedule and view it from the Admin Module Tab. Follow the given steps to add a schedule.

1. Click Add. It takes you to 'New Schedule' page.
2. Enter the Task Name.
3. Enter the Description of the Task.
4. By default the Status would be 'Enable'
5. Under Recurrence Details, Choose the time period for which monitoring is not needed. The Schedule can be Daily, Weekly or Random.
6. Select the Monitors for which monitoring is not needed from Monitors Details. On saving, the chosen Monitors would have their Maintenance Tasks scheduled.

Click on Downtime Scheduler View under Admin Module Tab. It takes you to 'Downtime Schedules' page. It displays information about the Monitors for which Maintenance Tasks have been scheduled. Edit Option is available to modify the schedule.
SNMP Trap Listener

SNMP Trap Listener can be configured in such a way that, if a particular trap is received, actions can be configured and alerts will be generated accordingly. For e.g., you can configure a trap listener for system shutdown, you can assign the severity as critical and also associate an email action through SNMP Trap Listener. If the trap is received, then the severity becomes critical and an email alert is generated.

The default port through which the traps are received is 1620. The default port can be changed by modifying <am.traplistener.port> property in <AMServer.properties> under AppManager6/Conf directory. Restart the server for the changes to take effect.

Follow the steps given below to add a SNMP Trap Listener.

1. Under Admin Tab, Click on 'Add' in SNMP Trap Listener. It takes you to 'Add SNMP Trap Listeners' page.
2. Enter the Trap Listener Name.
3. Status is 'enable' by default.
4. Select the SNMP Trap version
5. If the version is v1, then select the Generic Type. The various generic types are coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss, and enterpriseSpecific.
6. Enter the Enterprise OID. You can use the MibBrowser to get the Object ID
7. If the version is v2c, then enter the Trap OID. You can use the MibBrowser to get the Object ID
8. Select the Severity. It can be Clear, Warning or Critical.
9. Trap can be received from any Host or you can specify the Host from which the trap can be received.
10. Associated actions that need to be executed when the trap is received, can be chosen from the list of actions configured. Save the Trap Listener.

You can view the Traps by clicking on 'View' from the Admin Tab. It opens up to 'View SNMP Trap Listeners' page, in which details about the trap listeners are given. Edit option is available to modify the traps listeners. Also, the alerts configured for the traps received can be viewed from the Alerts Tab.
Schedule Reports

Applications Manager generates many reports that help you to analyze the performance over a period of time. Using this option, you can schedule the time at which the reports need to be generated.

To create New schedule of reports

1. Click on the Admin tab
2. Under Tools, click on Schedule Reports.
3. If reports have been already scheduled, the schedule details would be listed. Else, it would prompt you to create new schedule.
4. Give a name for the schedule
5. Enter the description of the schedule
6. By default, the schedule for the report is enabled.
7. Choose the Report Type like Availability report, Downtime history report.
8. Select the Report period.
9. Choose whether you want report for monitor group or for individual monitors. Accordingly, the resources will be listed down. Select the resource for which the report is expected.
10. Set the time for the reports to be delivered.
    For eg., If you want the Health report of database servers to be delivered everyday at 10.00 a.m, choose 'Daily' option and set the time as 10.00
    If you want the report to be delivered every monday at 10.00 a.m, choose 'Weekly' option, set time as 10.00 and choose 'Monday' option.
    If you want the report to be delivered every month on 15th day at 10.00 a.m, choose 'Monthly' option, set time as 10.00, choose 15 from the day list and select all for the report to be delivered every month. (you can select individual months also)
11. Select whether you want to receive the report as PDF files or as URL links.
12. If email actions are already configured, select the email to which the reports need to be sent else you can configure new email action.
13. Click 'save' to create the reports schedule.
Manager Console

Manager Console would essentially help the Manager to have an integrated high-level view of the Business Infrastructure. Here, monitor groups form Business Application units. The manager can create service level agreement (SLA), the violation of which can be escalated by Email.

The Manager Console gives the overall status of the various Business Applications that are associated with the system. You can view the availability statistics graph of the Business Applications for various time periods like 'Today', 'Yesterday', 'Last Week', 'This month', etc.,

The Service Level Agreement (SLA) statistics table lists all the Business Applications & their SLAs and indicates whether the SLAs have been met or not. You can view the Total Downtime, Availability % (clicking on the availability value will help you view the overall availability report of the Monitor Group and also the availability reports of the individual Monitors in the Monitor Group), Mean Time To Repair (MTTR), MTBF (Mean Time Between Failures).

Mean Time To Repair (MTTR): The average time to repair a device or a system back to acceptable operating conditions. The term can also mean, the time spent to restore a machine to operating condition after failure. This must be as low as possible.

Mean Time Between Failures (MTBF): The average time that a device or a system worked without failure. The term can also mean the length of time a user may reasonably expect a device or system to work before an incapacitating fault occurs. This must be as high as possible.

Server SLA:

Upon clicking the Server SLA tab, you can view the SLA details for all the servers associated. Server Availability statistics is shown as a pie chart. By default, the least availability statistics for 'Today' is shown. A maximum of availability details of 12 servers would be shown as pie chart. You have an option to view the availability statistics for other time periods like 'Yesterday', 'Last Week', 'Last month', etc.,

The server availability statistics - uptime % table, clearly lists down all the Servers associated with the different types of SLAs and it indicates whether the Servers have met the SLAs or not. If there is a SLA violation, the corresponding statistics is highlighted in red.

The other details that can be viewed are Total Downtime, Availability %, MTBR, MTBF along with the trouble tickets associated with it. You can view the Server availability report for the past seven days by clicking on the 7 Icon.

Trouble Tickets SLA:

Upon clicking the Trouble Tickets SLA tab, you can view the SLA details for all the trouble tickets associated. Trouble Ticket Volume statistics is shown as a bar graph. By default, the volume statistics for 'Today' is shown. A maximum of ticket volume details of 12 business applications would be shown as bar graph. You have an option to view the Trouble ticket volume statistics for other time periods like 'Yesterday', 'Last Week', 'Last month', etc.,

The Trouble Ticket Volume table, clearly lists down all the Business Applications associated with the different types of SLAs and it indicates whether trouble ticket volume has met the SLAs or not. If there is a SLA violation, the corresponding statistics is highlighted in red.

Across the various time periods, you can compare the trends in the volume of Trouble Tickets.

Creation of New Service Level Agreements:

- Click on the New SLA link
- Enter the SLA Name
• Enter the **SLA Description**
• Choose whether to use the SLA for **Business Application** or for **Server**
• Then you go on to define the SLA Rules
• The Service Level Objectives provided are **Availability** and **Trouble Tickets**
• To meet the SLA, Availability can be set as equal to, greater than, or greater than equal to a percentage value. By default it is 99.9 %
• To meet the SLA, the Trouble Ticket Volume can be set as less than, equal to or less than equal to a particular number of Trouble Tickets per month.
• The next step is to **associate the SLA to the Business Applications or the servers** as per the initial choice. From the available list, Select the Business Applications / Servers that you want to monitor using the SLAs.
• You have an option to escalate **SLA violation through Email**. Enter the From address, to address, subject, and message of the escalation Email. The mail will be sent to the recipient(s) with the root cause message of the SLA violation.
• Click on 'save' to create a new SLA.
Integrating with ServiceDesk Plus

ServiceDesk Plus is a web-based Help Desk and Asset Management software, offered by AdventNet.

If ServiceDesk Plus is installed in your network, you can automatically log trouble tickets for specific alerts, from Applications Manager. So, besides the provision to email, sms, and notification of alerts in other forms, the alerts can also be tracked by logging trouble tickets to ServiceDesk Plus. This helps in issue tracking.

For logging the trouble ticket to ServiceDesk Plus correctly, the following needs to be ensured:

- **Incoming Mail Settings** should be configured properly in ServiceDesk Plus
- **ServiceDesk Plus Settings** should be configured in Applications Manager.
- **Mail Settings** of Applications Manager must be configured.
- **Log a Ticket Action** should be configured
- **An alert should be associated** to the Ticket Action, to log a trouble ticket to ServiceDesk Plus
Technical Support and Product Information

Clicking 'Support' tab in the web client provides you the following information.

- Applications Manager Support
- User Forum Discussions
- Applications Manager Team Blog
- Testimonials
- Product Information
- Applications Manager Installation Information
- JVM Memory Information
- Database Connection Time
- Database Request Statistics
- System CPU Utilization
- System Response Time

Applications Manager Support

Request Technical Support

Clicking this link takes you to an online support form. Describe the problem, specify your name, e-mail ID, telephone number, and additional information if any and click Submit.

Alternatively, you can simply send an e-mail to support@appmanager.com.

Support Information File

For the Applications Manager Technical Center to resolve problems quickly, you need to send the log files that are being generated. To do so, click Support Information File link. The log files are zipped in a file and placed under <Applications Manager Home>/support directory. File creation takes some time based on the log file size.

To create Support Information File via Command Prompt, execute the following command:

```
<C:\ProgramFiles\AdventNet\ME\AppManager6\bin>createSupportFile
```

After generating the support information file, e-mail it to support@appmanager.com.

If the Support Information file is large in size and our mail server blocks the same, then you can upload the file in AdventNet's FTP site.

You will be provided details of the FTP service usage when you connect to our FTP server using "ftp ftp.adventnet.com"

Server Name = ftp.adventnet.com
user account = anonymous
password = "your email address"

Kindly email the location of the file and the folder in which it is placed in case you are using ftp to upload the file.
Troubleshooting Tips

Clicking this link takes you to the online Troubleshooting page which is a quick stop to get your problems resolved by yourself. This page quotes the common problems faced by users and provides a quick solution.

Toll Free Number

You can call the Toll Free Number +1-888-720-9500 and ask for assistance from the Applications Manager Technical Center.

Need Features?

If you would like to see more new features in Applications Manager, click the Need Features link. This takes you to an online form where you can specify the feature and its description.

User Forums

Clicking this link will take you to the online user forums where you can discuss about Applications Manager with other users. Five latest discussion topics will be displayed.

Applications Manager Team Blog

Clicking this link will take you to the online Applications Manager Team Blog where you can view interesting information about the team, tips on handling Applications Manager and many more. Five latest blogs will be displayed.

Testimonials

Clicking this link will take you to the online Testimonial form, wherein you can leave your feedback about Applications Manager.

Product Information

This sections provides the following information.

- **Product**: Name of the product.
- **Build Number**: Build number of the product currently installed in your machine.
- **Service Pack**: The service pack that has been currently installed over the product.
- **License Type**: Type of license that you are currently using (Free, Evaluation, Paid) and the number of days remaining if it is an evaluation edition.
- **Buy/Evaluate**: 'Buy' option is available if you are using an Evaluation edition. Click 'Buy' to go to the online store and purchase Applications Manager product license. 'Evaluate' option is available if you are using a Free Edition. Click 'Evaluate' to switch from Free edition to Evaluation edition (30 days).

Applications Manager Installation Information

This section provides information about the system where you have installed the product.

- **Host Name**: Host name where the server is running.
- **OS Type & Version**: Type and version of operating system of the host.
- **Working Directory**: Your working directory or Applications Manager Home (where the product is installed).
• **Start Time**: Time the server was started.
• **Server port**: Port in which Applications Manager is running
• **Number of Monitors**: Current number of monitors configured
• **Named Users**: Current number of users configured

**JVM Memory Information**

This section provides information on the JVM Memory usage.

• **Total JVM Heap Size**: Total heap size occupied by JVM.
• **Used JVM Heap Size**: Heap size used by JVM.
• **Free JVM Heap Size**: Heap size that is free without JVM usage.

**Database Connection Time**

This graph provides information on the Applications Manager database connection time for the last one hour.

**Database Request Statistics**

This graph provides information on the Applications Manager database request statistics for the last one hour.

**System CPU Utilization**

This graph provides information on the system's (where Applications Manager is installed) CPU Utilization pattern for the last one hour.

**System Response Time**

This graph provides information on the system's (where Applications Manager is installed) Response Time pattern for the last one hour.
### Glossary

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>These are tasks to be performed to notify the user, when alerts are generated by Applications Manager.</td>
</tr>
<tr>
<td></td>
<td><strong>For example</strong>, while monitoring WebLogic server, if the user wants to be intimated when the server response time is greater than 1000ms, then an alert is generated when the condition is met. The users are notified of the alerts through Actions such as sending e-mail, SMS, trap, and executing a command.</td>
</tr>
<tr>
<td><strong>Admin Activities</strong></td>
<td>Activities allowing IT administrators to configure any operation in Applications Manager with ease. Only the ‘Admin’ user can perform these activities. For more information on user access, refer to the User Administration section.</td>
</tr>
<tr>
<td><strong>Alerts</strong></td>
<td>Alerts are notifications generated based on Threshold / Health values. They are generated when the value of a numerical attribute exceeds the pre-defined threshold limit. Additionally, the status of health and availability of an application can also be determined through alerts.</td>
</tr>
<tr>
<td><strong>Alert Configuration</strong></td>
<td>This activity enables the user to associate a threshold profile with an attribute so that alerts are generated. It includes associating the action to be executed when an alert is generated. Additionally, the dependencies for the ‘Health’ attribute of a Monitor can also be configured.</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>Attributes are parameters/objects of a Monitor and they provide information about them. These are parameters whose values are set to threshold to generate alerts.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>An attribute that determines whether a system or application is available for use (Up or Down).</td>
</tr>
<tr>
<td></td>
<td><strong>For example</strong>, If a Web server is running, then the availability is up.</td>
</tr>
<tr>
<td></td>
<td>Consider a situation where the Web server may be running fine but its response time is high. This is indicated by Availability as Up and Health as critical if the response time is a dependent parameter for health.</td>
</tr>
<tr>
<td><strong>Monitor Groups</strong></td>
<td>Refers to the logical grouping of one or more Monitors such as application servers, network services, databases, web applications etc. This provides a holistic view of the business environment.</td>
</tr>
<tr>
<td><strong>Custom Monitor</strong></td>
<td>Custom Monitors provide a way to monitor your Java applications or other applications that expose management information through SNMP (Simple Network Management Protocol) and JMX (Java Management Extensions). Say, you have a Java application with built-in manageability using JMX and any application that has an SNMP interface, then they are managed by building Custom Monitors.</td>
</tr>
<tr>
<td><strong>Dependencies</strong></td>
<td>Dependencies determine • health of Monitor or Monitor Group • health or availability of Monitor Group They consist of the dependent parameters of the Monitor based on which the severity of the health and availability is determined.</td>
</tr>
<tr>
<td></td>
<td><strong>For example</strong>, Health of a Tomcat Server may depend on the overall response time of the server or on the response time of each of the web applications deployed on the server etc. By configuring dependencies, you can determine the attribute, based on which the severity of health changes.</td>
</tr>
</tbody>
</table>
### Terms and Definitions

<table>
<thead>
<tr>
<th><strong>Terms</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discover Network</strong></td>
<td>Locating all Monitors running within a network range.</td>
</tr>
<tr>
<td><strong>Enterprise OID in SNMP Trap</strong></td>
<td>OID that uniquely distinguishes traps of different organizations, i.e. they vary for different vendors. This field applies only to SNMPv1 traps.</td>
</tr>
<tr>
<td><strong>Generic Type in SNMP Trap</strong></td>
<td>These are types that are mapped to specific OID to generate SNMP traps and provide additional information about the functioning of the Monitor Group. They are applicable only to SNMPv1 traps. The different types of Generic traps are coldStart, warmStart, linkDown, linkUp, authenticationFailure, and egpNeighborLoss.</td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>An attribute that indicates the quality of Monitors, based on their dependencies. <strong>For example</strong>, if a Web server takes 10 mins to respond, its response time is high but the server is still available. Hence it is indicated by Health as critical (if response time is a dependent parameter of health) and <strong>Availability</strong> as up.</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>It is a continuous process that uses methodical collection and analysis of data to provide business management.</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>Application on which monitoring is performed. Monitor is an instance of a Monitor Type that is running in a port of a host. <strong>For example</strong>, Application Servers such as WebLogic servers or Tomcat servers etc, Database servers such as Oracle or MySQL servers are some of the Monitor Types while a WebLogic server running on a particular port of a host is a Monitor.</td>
</tr>
<tr>
<td><strong>Monitor Type</strong></td>
<td>Refers to application such as WebLogic server, JBoss server, System server, URL Monitor, Oracle Database server, MySQL Database server, etc. that are monitored by Applications Manager. Different instances of these applications are Monitor.</td>
</tr>
<tr>
<td><strong>Mean Time To Repair (MTTR)</strong></td>
<td>The average time to repair a device or a system back to acceptable operating conditions. The term can also mean, the time spent to restore a machine to operating condition after failure. This must be as low as possible. MTTR thresholds can be set to trigger root cause.</td>
</tr>
<tr>
<td><strong>Mean Time Between Failures (MTBF)</strong></td>
<td>The average time that a device or a system worked without failure. The term also stands for the length of time a user may reasonably expect a device or system to work before an incapacitating fault occurs. This must be as high as possible. MTBF thresholds can be set to trigger root cause.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>The time interval to monitor the different parameters configured for a Monitor.</td>
</tr>
<tr>
<td><strong>RCA</strong></td>
<td>Root Cause Analysis helps to point the actual cause of a problem. You can view the ‘Root Cause Analysis’ by clicking on the status icon of the attributes. <strong>For example,</strong></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Health of System" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Health of mapi-solaris1" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Physical Memory Utilization of mapi-solaris1" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Health of app-solaris1" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Swap Memory Utilization of app-solaris1" /></td>
</tr>
<tr>
<td>Terms</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Expand the nodes</td>
<td>To view the actual cause of the problem. Here, WebLogic Health is critical as Availability and Response Time (dependencies of Health) are also critical.</td>
</tr>
<tr>
<td>Reports</td>
<td>They provide organized presentation of data that depicts the behavior of Monitor Types over a specified period of time.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The time taken by a Monitor to react to a given input.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates how serious the problems are. There are three levels of severities: Critical, Warning, and Clear. These are controlled by the threshold set by the user or administrator.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>An outgoing e-mail server using Simple Mail Transfer Protocol (SMTP) that sends your outgoing messages to the appropriate recipients. Most e-mail systems that send mail over the Internet use SMTP to send messages. The messages can be retrieved using POP server.</td>
</tr>
<tr>
<td>SNMP OID</td>
<td>Object identifier (OID) that is used to uniquely identify each object variable of a MIB (Management Information Base).</td>
</tr>
<tr>
<td>Specific Type in SNMP Trap</td>
<td>When generic is set to Enterprise, a specific trap ID is identified.</td>
</tr>
<tr>
<td>SubNetMask</td>
<td>The subnet mask determines the maximum number of hosts on a subnetwork.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Threshold is the value that determines the severity of the alert based on the pre-defined conditions.</td>
</tr>
<tr>
<td></td>
<td><strong>For example</strong>, if the user wants to be intimated when the server response time is greater than 1000ms, then a threshold can be created based on this condition and assigned to the attribute.</td>
</tr>
<tr>
<td>URL Monitors</td>
<td>Continuous URL monitoring service that monitors web pages. They verify the availability of specified, addressable, standard HTTP and HTTPS URLs of web pages.</td>
</tr>
</tbody>
</table>
FAQ

General
1. What can ManageEngine™ Applications Manager do?
2. Can I create additional users to access Applications Manager?

Monitoring
1. What is the difference between Monitor Type and Monitor?
2. Does Applications Manager support monitoring of multiple Monitors in a single machine?
3. Can I discover all the services running in a particular range of network?
4. How do I view the Monitors discovered in the network?
5. Can I change the polling interval of a Monitor?
6. What does the 'New Monitor' do?
7. Is it required to associate a Monitor with a Monitor Group for monitoring?
8. Can a single monitor be associated with multiple Monitor Groups?
9. Does all the Monitor running in a particular server or host also get discovered, while discovering the Monitor? What must be done to discover all the Monitor?
10. While discovering a Monitor, the server in which the Monitor is running also gets added to my Monitor Group. Do I have an option to disable the same?
11. Do I have an option to view the history of data of any Monitor?
12. Is it possible to monitor Java applications that exposes information through SNMP or JMX? Can the JMX agent generated by AdventNet ManageEngine™ JMX Studio be monitored using Applications Manager?
13. What are the steps involved in managing a custom monitor?
14. What does the URL Monitoring do?
15. What is the difference between HTTP-URL and HTTP-URL Sequence monitoring?
16. Can I use my own database to dump data?
17. I have Tomcat 3.x version. How can I add a graphic about "Threads Availability" to my Tomcat monitor?
18. Which ports are going to be taken up by Applications Manager on startup? Do I have an option to modify the default ports?
19. Is it possible to monitor a SQL Server 2000 server only installed as an instance?
20. I've configured Monitors and created actions and threshold profiles in one of my machines, say Beta. Is there a way to export this data (alerts, monitors & threshold profiles) to some file, which can then be imported onto another application manager in the deployment server?
21. Is it possible to add the network interfaces data (e.g different SNMP MIB Data) into Application Manager?
22. Is it possible to keep the data more than 1 month, (e.g. 1 year) to be used as an historical/capacity planning database?
23. Once the server starts, the web client login page is automatically displayed in an already open browser. How do I disable this? I prefer to open the web client myself.
24. What happens when I start Applications Manager with different system user names?
25. What are the ports to be opened, when Applications Manager is running in a machine which is behind a firewall?
26. What are the different ways to monitor Custom Applications?
Alerts

1. How do I associate the threshold profile and actions, once i create them?
2. Can threshold be associated with both numerical and string attributes?
3. What determines the severity of health and availability? Is threshold related to health and availability?
4. When does health of a monitor become critical? How are actions affected?
5. Is it possible to view all the threshold and actions configured for different Monitors present in a particular Monitor Group?
6. How do I find out the cause for the severity of every attribute?
7. Can I associate a Monitor with a new threshold or actions?
8. Is there an option to edit the threshold or actions?
9. In Alerts screen, do i have an option to view only 'Critical' alerts?

Miscellaneous

1. I have my own web applications and other Java applications, but they do not expose management information using JMX or SNMP. What should I do?
2. I have some of my native (non Java) applications, but they do not expose management information using SNMP. What should I do?
3. How can I make an ODBC Connection with Applications Manager DB and then query it with crystal reports ??
4. How can I change the language of Applications Manager after installation?

General

1. What can ManageEngine™ Applications Manager do?

AdventNet ManageEngine™ Applications Manager helps to monitor your applications such as Web applications, application servers, Web servers, databases, network services, systems, etc. That is, it helps you to identify and analyze faults and performance issues in your applications well in advance.

2. Can I create additional users to access Applications Manager?

Yes. You can add more users apart from the default 'admin' user. For more information on creating a user access, refer to the User Administration section.

Monitoring

1. What is the difference between Monitor Type and Monitor?

Application servers such as WebLogic server, JBoss server, etc. and Database Servers such as Oracle Database server, MySQL Database server, etc. that are monitored by Applications Manager are called Monitor Type.

Different instances of these Monitor Types running on a particular port of a host are called Monitor.

2. Does the Applications Manager support monitoring of multiple Monitors in a single machine?

Yes, it supports monitoring of multiple Monitors in a single machine.

3. Can I discover all the Monitors running in a particular network?

Yes, you can discover all the Monitors running in a particular network. For more information, refer to the Discover Network section.
4. How do I view the Monitors discovered in the network?

Once you create the Monitor, they can be viewed by clicking the Monitors tab. This lists the Monitor Type and the number of Monitors created in the Applications Manager. Refer to the Monitor Information section for more information.

5. Can I change the polling interval of a Monitor?

Yes, you can change the polling interval using the Edit Monitor option. Refer to the Reconfiguration Details section for more information.

6. What does the 'New Monitor' do?

This option is used to create a new Monitor where the Monitor is discovered from the network and also to collect data (performance metrics, availability etc).

7. Is it required to associate a Monitor with a Monitor Group for monitoring?

A Monitor need not be associated with a Monitor Group for monitoring. Once the Monitor is created, Applications Manager starts monitoring it irrespective of whether the Monitor is added to the Monitor Group.

The purpose of associating a Monitor with a Monitor Group is to provide a holistic view to your Monitor Group.

8. Can a single Monitor be associated with multiple Monitor Groups?

Yes. A Monitor can be associated with multiple Monitor Groups using the Associate Monitor option. Follow the given steps:

1. Click on the Monitor Group. You will find Associate Monitor in the left frame under the Application Links section.
2. Move the mouse over it and click on the Monitor Type. It will list its respective Monitor.
3. Select Monitor and click Finish.

Similarly, you can add the same Monitor to another Monitor Group by following the above steps.

9. Does all the Monitors running in a particular server or host also get discovered while discovering the Monitor? What must be done to discover all the Monitors?

When a server or host is discovered, all the Monitors running in it will not be discovered. In case you want to discover all the Monitor running in a server or host, use the All Services option in the Create New Monitor screen. Refer to the Discovering All Monitors in a Host section for more information.

10. While discovering a Monitor and adding it to my Monitor Group, the server in which the Monitor is running also gets added to my Monitor Group. Do I have an option to disable the same?

Yes. Using Global Settings option, you can add a Monitor to your Monitor Group without the server or the host getting added to it by default, Refer to the Global Settings section for more information.

11. Do I have an option to view the history of data of any Monitor?

Applications Manager archives the data for every one hour. The data can be viewed from the Reports tab. The data is archived for particular attributes of the Monitor. Refer to the Grouping Reports chapter for more details.

Additionally, you can also view the past 7 and 30 days report by clicking the 7 and 30 icon respectively, available in every graph of Monitor.
12. Is it possible to monitor Java applications that expose information through SNMP or JMX? Can the JMX agent generated by AdventNet ManageEngine™ JMX Studio be monitored using Applications Manager?

Yes. Custom Monitors provide a way to monitor your Java applications that expose management information through SNMP or JMX. Hence, Custom Application can be used to monitor AdventNet JMX agent.

13. What are the steps involved in managing a JMX or SNMP resource using CAM?

Building Custom Monitor involves:

- Creating Custom Monitor and adding it to a specific Monitor Group
- Adding Attributes

14. What does the URL Monitoring do?

URL Monitoring tests the web pages to ensure that they are functioning properly. It supports monitoring of standard HTTP and HTTPS URLs of web pages. Refer to the HTTP URL Monitors for more information.

15. What is the difference between HTTP-URL and HTTP-URL Sequence monitoring?

The difference between the two types of monitoring is that HTTP-URL monitors single HTTP and HTTPS URL, whereas HTTP-URL sequence monitors a set of HTTP and HTTPS URLs invoked in sequence.

Also, any HTTP and HTTPS URL can be monitored using HTTP-URL, provided they require no authentication details.

16. Can I use my own database to dump data?

When starting Applications Manager, MySQL Server 4.0.20, which is bundled with the product, is started. Applications Manager uses this MySQL by default. We strongly recommend you to use this default database itself. If you need to dump data into your own database in that same machine, follow the steps given below.

1. Edit the database_params.conf file located in the <Applications Manager Home>/working/conf directory and change the following URL.

   Default URL: jdbc:mysql://localhost:13326/AMDB

   Change to: jdbc:mysql://<HOSTNAME>:<PORT>/<DATABASE>

2. Edit the startApplicationsManager.bat/.sh located in the <Applications Manager Home> directory and comment out the MySQL starting part. Search for the string "startMySQL" and comment out that line. As we are using the MySQL installed in the same machine, there is no need to start the MySQL Server bundled with the Applications Manager.

3. Start the Applications Manager. Note: When starting Applications Manager, you will get a warning message MySQL Port is used by some other Application. You can ignore this message.

17. I have Tomcat 3.x version. How can I add a graphic about "Threads Availability" to my Tomcat monitor?

The data for the "Threads Availability" will be shown only for 5.x versions of the Tomcat Server. This data is not available for 3.x and 4.x version of Tomcat Server. For more information on the data that is displayed for each of the Tomcat versions, refer to the Tomcat Servers topic.
18. Which ports are going to be taken up by Applications Manager on startup? Do I have an option to modify the default ports?

Web Server : 9090  
MySQL : 13326  
RMI port : 11099  
WEBCONTAINER_PORT : 18009  
TOMCAT_SHUTDOWNPORT : 8006  
TCP_PORT : 12000  

To modify the default port, edit the file AMServer.properties located in the <Applications Manager Home>/conf directory and modify the required ports. Restart the server for the changes to take effect.

**Note:** You will want to edit only the Web Server Port as it is required to connect to the Web Client. For other ports, Applications Manager automatically finds the available ports and connects to it at startup.

**Important:** When editing web server port, ensure if you have installed the Applications Manager as a Windows service. If installed so, you need to change the web server port in yet another file (apart from AMServer.properties) httpd.conf located in <Applications Manager Home>/working/apache/conf. Set the new web server port for the Listen parameter in this file.

19. Is it possible to monitor a SQL Server 2000 server only installed as an instance?

SQL Enterprise manager uses: [servername]\[instancename]

For monitoring MS SQL 2000 Server, you have to specify the Host Name or IP Address of the machine in which MS SQL Server is running.

What is shown in Enterprise Manager is [servername]\[instancename]. Here servername refers to the machine in which the MS SQL 2000 Server is running and instancename refers the name of the MS SQL 2000 Server. Hence while adding the MS SQL 2000 server, you have to specify only the servername part in the Hostname / IP Address field and not the instancename.

20. I've configured Monitors and created actions and threshold profiles in one of my machines, say Beta. Is there a way to export this data (alerts, monitors & threshold profiles) to some file, which can then be imported onto another application manager in the deployment server?

1. Applications Manager is data driven and all data is in a mysql database. You can copy the <Applications Manager Home>/working/mysql/data/AMDB folder and replace the one in the new installation in the production system.

2. Delete the files befailover.frm, befailover.MYD and befailover.MYI located in the AMDB folder before using it for an AM instance running in a different machine. These files contains entry for the hostname of the machine in which AM is installed.

3. Start the server.

**Note:**
- Ensure that there must be no date and time difference between the 2 hosts as this may affect the Reports that were created / alerting mechanism.
- The above suggestion will work for moving data between:
  - Linux to Linux
  - Windows to Windows
  - Linux to Windows

Besides, it is best that the Beta machine and the target host have the same operating system. Also, shutdown the Applications Manager before doing this. Applications Manager should be shutdown using the shutdownApplicationsManager.sh/.bat scripts only.
21. Is it possible to add the network interfaces data (e.g. different SNMP MIB Data) into Application Manager?

You can achieve this by creating Custom Applications. For more information, refer to Adding SNMP OID Attributes topic.

22. Is it possible to keep the data more than 1 month, (e.g. 1 year) to be used as an historical/capacity planning database?

Yes, you can view historical reports of more than a month (apart from the daily, 7 days, and 30 days reports). For example, if you have data collected for more than a month or a year, you can view historical reports for a particular day or a range of days using the 'Custom Time Period' option. For more information, please refer to Viewing Reports topic.

23. Once the server starts, the web client login page is automatically displayed in an already open browser. How do I disable this? I prefer to open the web client myself.

Yes, you can disable this automatic action. Edit AMServer.properties file located in the <Applications Manager Home>/conf directory and set the am.browser.startup parameter as false. After this configuration, when you restart the server, you will need to manually invoke the web client.

24. What happens when I start Applications Manager with different system user names?

For example, you have installed Applications Manager in a system with user access as 'admin'. The Applications Manager server is started. The <Applications Manager Home>/working/mysql/data/AMDB folder files are set with 'admin' permissions. In a later period you have logged into the system using another user name, say 'guest', and started Applications Manager. At this point, the AMDB files are set with the 'admin' permission. Because of the change in file permissions, there will be malfunctioning of the monitors and when Alerts tab is clicked, exceptions might be thrown.

To avoid this error, you need to ensure that the same user login is used everytime you start Applications Manager in your system. If you have AMDB files with different user permissions, perform the following steps to change all permissions to a single user permission.

1. Login to system with a user name that you need to reset, say 'admin'.
2. Go to <Applications Manager Home>/working/mysql/data/AMDB directory.
3. Execute the following command.
   chown -R <the user name that is to be reset> *
   Example: chown -R guest *
4. Restart the Applications Manager.
5. Also make sure you start the Applications Manager from /etc/rc.local file as 'guest' user.

On performing this, all the files under <AMDB> directory is set with 'guest' permission.

25. What are the ports to be opened, when Applications Manager is running in a machine, which is behind a firewall?

Refer to Configuring Secure Applications Manager topic for details on what ports need to be opened when there is a firewall.

26. What are the different ways to monitor Custom Applications?

- If SNMP is enabled in that application, you can use SNMP monitor to monitor that particular application. Also if you have Mib for your application, you can upload that mib to applications manager and add the required attributes to be monitored.
• If your applications java and exposes data through JMX or it uses JDK 1.5 and exposes data through JMX, you can use JMX [MX4J / JDK1.5] monitor to monitor your application and also add required attributes for monitoring exposed by JMX.

• If the custom application is running in a particular TCP port, you can use Service monitoring to monitor the port and check for availability of that port.

• If the application is web based application (like IIS or Apache), you can use HTTP-URLs and HTTP-URL Sequence monitoring to monitor the URLs for their availability.

• If you have a script in Applications Manager machine which can monitor your application, Applications Manager server can execute this script periodically using Script monitor. It will also generate reports and escalate alerts according to the results obtained.

• If you have a web application running over JDK 1.5, you can use Web Transaction Monitor to monitor the end to end details about the application. Please refer the following link for details, Web Transactions

alerts

1. How do I associate the threshold profile and actions, once I create them?

Thresholds and actions can be associated using Configure Alert option. Refer to the Associating Threshold and Actions with Attributes section.

2. Can threshold be associated with both numerical and string attributes?

Yes. Threshold can be associated with both numerical and string attributes.

3. What determines the severity of health and availability? Is threshold related to health and availability?

The child Monitors or sub-components (also called 'dependencies') determine the availability and severity of health for a Monitor Group or Monitor.

Health: The health is based on the severity of the attributes that are added as its dependencies. The severity of the attributes is in turn dependent on the Threshold. Hence the threshold is indirectly related to health.

Availability: The availability of a Monitor Group is dependent on the availability of its Monitor. The availability of Monitor is determined during discovering the Monitor and it is internally handled. Hence threshold is not related to the availability.

Refer to the Configuring Dependencies section for details on dependencies.

4. When does health of a monitor become critical? How are actions affected?

The child Monitors or sub-components (also called 'dependencies') determine the availability and severity of health for a Monitor Group or Monitor.

Health of the Monitor: The health is based on the severity of the attributes that are added as its dependencies. The severity of the attributes is in turn dependent on the Threshold. By default, if any one of the dependencies is critical, the health of the monitor becomes critical. The user has an option to choose the dependencies that affect the health of the monitor. Refer to the Configuring Dependencies section for details on dependencies.

The Actions associated would be executed only if there is a change in the severity. For eg., if the health of the monitor changes from clear state to critical state, an alert is generated and the action associated would be executed, say an email alert would be sent to the user.
5. Is it possible to view all the thresholds and actions configured for different Monitors present in a particular Monitor Group?

Yes. You can use the **Global Alert Configuration** option to view all the thresholds and actions configured for all Monitors of a particular Monitor Group. Refer to the **Viewing and Configuring Alerts Globally** for more information.

6. How do I find out the cause for the severity of every attribute?

You can view the cause for the severity of every attribute using the **Root Cause Analysis** option. Click on the severity icon and expand the node to view the cause. Refer to the **Root Cause Analysis** section of Glossary.

7. Can I associate a Monitor with a new threshold or actions?

Yes. You can associate the Monitor with a new threshold by using the **Configure Alert** option available for every attribute of the Monitor. In **Configure Alert** screen, choose the new threshold and save the changes.

You can also do the same through the **Global Alert Configuration** screen by following the given steps:

1. Click on the Monitor Group.
2. Click on the **Global Alert Configuration** from the left frame. This lists all the Monitors and their associated thresholds and actions.
3. Click the **Edit** icon of the Monitor whose threshold must be changed. This opens the **Configure Alert** screen.
4. Select the new threshold from the combo box of Associate Threshold.
5. Click **Save All**.

This changes or associates the new threshold with the Monitor. You can also follow the same steps to associate actions.

8. Is there an option to edit the threshold or actions?

Yes. Go to **View Threshold**. This lists all the threshold profiles and their details. Click the **Edit** icon and make the changes. To edit an action, follow the same steps in **View Actions**.

9. In Alerts screen, do I have an option to view only 'Critical' alerts?

Yes. Click on the **Alert Summary** icon. A dialog with the recent critical alerts pops up. To view all the critical alerts, click on the **Critical part of the graph**. This lists all the critical alerts in the **Alerts** screen. The same steps can be followed to view alerts for other severity.

**Miscellaneous**

1. I have my own web applications and other Java applications, but they do not expose management information using JMX or SNMP. What should I do?

AdventNet offers **ManageEngine JMXStudio** that can help build manageability into your software by exposing information through JMX and its various adapters such as SNMP, SOAP, AMI, RMI, etc.

2. I have some of my native (non-Java) applications, but they do not expose management information using SNMP. What should I do?

AdventNet offers **AgentToolkit C Edition** that can help build manageability into your software by exposing information through management protocols such as SNMP, etc.
3. How can I make an ODBC Connection with Applications Manager DB and then query it with crystal reports?

You can make ODBC connection from localhost, that is you can make connection from the machine where Applications Manager is running. If you want to access mysql from remote machine, you have to give permission in user tables.

Connect to mysql and execute following commands,

```
INSERT INTO user (Host,User,Password) VALUES('host name with domain name','root',PASSWORD('appmanager'));
GRANT ALL PRIVILEGES ON *.* TO 'root'@'host name with domain name';
FLUSH PRIVILEGES;
```

For eg.,
```
INSERT INTO user (Host,User,Password)
VALUES('appmanager.adventnet.com','root',PASSWORD('appmanager'));
GRANT ALL PRIVILEGES ON *.* TO 'root'@'appmanager.adventnet.com';
FLUSH PRIVILEGES;
```

4. How can I change the language of Applications Manager after installation?

To change the language from the one that you have already installed,
- Go to `<AMServer.properties>` file found under `<Applications Manager Home>/conf`
- Edit the existing entries
  - For Japanese, put the entries as
    - `<am.server.language=ja>`
    - `<am.server.country=JP>`
  - For Chinese, put the entries as
    - `<am.server.language=zh>`
    - `<am.server.country=CN>`
  - For English, put the entries as
    - `<am.server.language=en>`
    - `<am.server.country=US>`
- Save and then restart Applications Manager.
Appendix

- A: Applications Manager Home
- B: Icon Representation
- C: Alert Details
- D: Reconfiguration Details
- E: Network View
- F: Miscellaneous Links Details
- G: Data Collection - Host Resource
- H: SNMP Agent Installation
- I: SNMP Agent Configuration
- J: Security/Firewall Requirements
Applications Manager Home

\textit{<Applications Manager Home>} refers to the directory in which you have installed the Applications Manager product. This directory location is specified by you when you install the product.

For example, let us assume that you have installed Applications Manager under the default \textit{<Program Files>} directory of C drive in your system. In this case, \textit{<Applications Manager Home>} denotes \texttt{C:\Program Files\AdventNet\ME\AppManager6}. In Linux, if Applications Manager is installed under home directory, then \textit{<Applications Manager Home>} denotes \texttt{~/AdventNet\ME\AppManager6}. 
## Icon Representation

The following are the icons used in Applications Manager and their significance:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Signifies</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Health is Critical" /></td>
<td>Health is Critical</td>
</tr>
<tr>
<td><img src="image" alt="Health is Warning" /></td>
<td>Health is Warning</td>
</tr>
<tr>
<td><img src="image" alt="Health is Clear" /></td>
<td>Health is Clear</td>
</tr>
<tr>
<td><img src="image" alt="Health Unknown" /></td>
<td>Health Unknown</td>
</tr>
<tr>
<td><img src="image" alt="Availability Down" /></td>
<td>Availability Down</td>
</tr>
<tr>
<td><img src="image" alt="Availability Up" /></td>
<td>Availability Up</td>
</tr>
<tr>
<td><img src="image" alt="Health of Numerical Attribute is Critical" /></td>
<td>Health of Numerical Attribute is Critical</td>
</tr>
<tr>
<td><img src="image" alt="Health of Numerical Attribute is Warning" /></td>
<td>Health of Numerical Attribute is Warning</td>
</tr>
<tr>
<td><img src="image" alt="Health of Numerical Attribute is Clear" /></td>
<td>Health of Numerical Attribute is Clear</td>
</tr>
<tr>
<td><img src="image" alt="Health of Numerical Attribute is Unknown" /></td>
<td>Health of Numerical Attribute is Unknown</td>
</tr>
</tbody>
</table>

### Monitor Type

<table>
<thead>
<tr>
<th>Icon</th>
<th>Signifies</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="JBoss" /></td>
<td>JBoss Server</td>
</tr>
<tr>
<td><img src="image" alt="Tomcat Server" /></td>
<td>Tomcat Server</td>
</tr>
<tr>
<td><img src="image" alt="WebLogic Server" /></td>
<td>WebLogic Server</td>
</tr>
<tr>
<td><img src="image" alt="WebSphere Server" /></td>
<td>WebSphere Server</td>
</tr>
<tr>
<td><img src="image" alt="Oracle Application Server" /></td>
<td>Oracle Application Server</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft .NET" /></td>
<td>Microsoft .NET</td>
</tr>
<tr>
<td><img src="image" alt="Web Transactions" /></td>
<td>Web Transactions</td>
</tr>
<tr>
<td><img src="image" alt="Apache" /></td>
<td>Apache</td>
</tr>
<tr>
<td><img src="image" alt="IIS Server" /></td>
<td>IIS Server</td>
</tr>
<tr>
<td><img src="image" alt="PHP" /></td>
<td>PHP</td>
</tr>
<tr>
<td><img src="image" alt="JMX [MX4J / JDK 1.5]" /></td>
<td>JMX [MX4J / JDK 1.5]</td>
</tr>
<tr>
<td><img src="image" alt="Exchange Server" /></td>
<td>Exchange Server</td>
</tr>
<tr>
<td><img src="image" alt="Mail Server" /></td>
<td>Mail Server</td>
</tr>
<tr>
<td><img src="image" alt="Service Monitoring" /></td>
<td>Service Monitoring</td>
</tr>
<tr>
<td><img src="image" alt="AdventNet JMX Agent - RMI Adapter" /></td>
<td>AdventNet JMX Agent - RMI Adapter</td>
</tr>
<tr>
<td><img src="image" alt="SNMP" /></td>
<td>SNMP</td>
</tr>
<tr>
<td><img src="image" alt="Web Server" /></td>
<td>Web Server</td>
</tr>
<tr>
<td><img src="image" alt="MySQL Database Server" /></td>
<td>MySQL Database Server</td>
</tr>
<tr>
<td><img src="image" alt="Oracle Database Server" /></td>
<td>Oracle Database Server</td>
</tr>
<tr>
<td><img src="image" alt="MS SQL Database Server" /></td>
<td>MS SQL Database Server</td>
</tr>
<tr>
<td><img src="image" alt="IBM DB2 Database Server" /></td>
<td>IBM DB2 Database Server</td>
</tr>
<tr>
<td><img src="image" alt="Custom Monitor" /></td>
<td>Custom Monitor</td>
</tr>
<tr>
<td><img src="image" alt="HTTP-URL Monitor and Sequence" /></td>
<td>HTTP-URL Monitor and Sequence</td>
</tr>
<tr>
<td><img src="image" alt="Linux Server" /></td>
<td>Linux Server</td>
</tr>
<tr>
<td><img src="image" alt="AIX Server" /></td>
<td>AIX Server</td>
</tr>
<tr>
<td><img src="image" alt="HP-Unix Server" /></td>
<td>HP-Unix Server</td>
</tr>
<tr>
<td><img src="image" alt="Solaris" /></td>
<td>Solaris</td>
</tr>
<tr>
<td><img src="image" alt="Windows Server" /></td>
<td>Windows Server</td>
</tr>
<tr>
<td><img src="image" alt="FreeBSD Server" /></td>
<td>FreeBSD Server</td>
</tr>
<tr>
<td>Icon</td>
<td>Signifies</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td>![icon]</td>
<td>Unknown</td>
</tr>
<tr>
<td>![icon]</td>
<td>Script Monitor</td>
</tr>
<tr>
<td>![icon]</td>
<td>QEngine Script Monitor</td>
</tr>
</tbody>
</table>

**Report**

- ![icon] 7
  - Report generated by monitoring the attribute of the Monitor for 7 days.
- ![icon] 30
  - Report generated by monitoring the attribute of the Monitor for 30 days.

**General**

- ![icon] Edit icon to make changes in the configurations.
- ![icon] Alert Configuration icon where the thresholds and actions of the attributes are associated with the Monitor/ Monitor Group.
Alert Details

Root Cause Analysis (RCA)

Based on the threshold and dependencies associated with the attributes of Monitor, the severity of the Monitor and Monitor Group is determined. You can view the Root Cause Analysis report by clicking the status icon of the attributes (Refer to the Icon Representation section of Appendix, to know the different status icons). Expand the nodes to view the actual cause of the problem.

The following are the quick links that can be viewed in Alerts page.

<table>
<thead>
<tr>
<th>All</th>
<th>Lists all the alerts based on Alert Views where there are options to choose a particular or all Monitor Groups and Monitor Types.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Lists all the alerts with status as critical. You also have the same options to choose a particular or all Monitor Groups and Monitor Types.</td>
</tr>
<tr>
<td>Last One Hour</td>
<td>Lists all the alerts generated for the last one hour.</td>
</tr>
<tr>
<td>Last One Day</td>
<td>Lists all the alerts generated for the last one day.</td>
</tr>
</tbody>
</table>

Recent 5 Alerts

Lists the recent 5 alerts generated by the Monitor that contains the following details:

- **Status**: Indicates the severity of the Monitor based on its pre-defined threshold.
- **Monitor Name**: Name of the Monitor that created the alert.
- **Message**: Refers to the problem that caused the alert. Click on the message to know more about the alert details. Also view the Alert History that gives you a detailed idea on generation of the alert and its status.
- **Time**: Time at which the alert is generated.

Alerts Summary

Lists the recent critical alerts of Applications Manager.
Reconfiguration Details

All the configuration details of the Monitor/ Monitor Groups are editable. To edit the Monitor Group details, use the Edit icon and to edit the configuration details of the Monitor, use the Edit Monitor link provided in the right frame of every Monitor.
Network View

This lists all the networks discovered for the Monitor of all the Monitor Groups. You have an option to view all the Monitors discovered in the network (All Networks) and also Monitors discovered within a specific network.

You can click on the Network IP address provided under Network View to view the number of Monitors discovered in that specified network range. To know more information on how to discover Monitor within a given range, refer to the Discover Network section of Performing Admin Activities.
Miscellaneous Links Details

The following are the links that are common throughout all the screens in the Applications Manager:

- **Quick Note**: Provides a brief description about the functioning of the different parameters on which you are currently working.
- **Talk Back**: You can send your technical feedback about Applications Manager by filling up the form.
- **About**: You can see the details of Applications Manager like Build No, SP version, type of license etc., and also the credits roll of the contributors to the product.
- **Personalize**: Provides an option to view the Applications Manager with a different look and feel, as you prefer. For more details, refer to the **Personalize** section of Performing Admin Activities.
- **Register**: You can apply the registered License file that you have purchased, by clicking on this link.
- **Help**: Provides detailed information about working with the product. Note that the help is context sensitive and you can click on the **Home** link to view the main page of Applications Manager Help Docs.
- **Logout**: To log out and return to login page.
- **Search**: The **Search Field** is placed on the left side and in all pages of the web client. It provides an option for searching relevant links for some keywords in the product. The keyword-specific links are categorized as Monitors, Help Documents, Bookmarks (pre-defined), and Reports that list the links under their respective category based on the keyword. For example, searching for keywords such as **Monitors** provide the relevant links under Help Documents and Bookmarks and for **WebLogic**, the links are categorized under Help Documents, Bookmarks, and Reports.

- **Alert Summary**: Lists the recent critical alerts of Applications Manager. You can also click on the shades (representing the different severity) in the graph that will display the alerts based on the severity.
- **Printer Friendly**: This option is available in all the pages of the web client. Clicking this link provides you a printer friendly view of the current page. This comes handy for printing Alerts and Reports.

*Note*: By clicking on **Jump to** link, you can choose to log into ManageEngine OpManager or ManageEngine ServiceDesk Plus from Applications Manager console itself, provided Applications Manager is configured in the chosen product.
### Data Collection - Host Resource

The important configuration details that are required while discovering host resource by Applications Manager are as follows:

<table>
<thead>
<tr>
<th>Applications Manager Operating System</th>
<th>Linux</th>
<th>Sun Solaris</th>
<th>HP-UX / Tru64</th>
<th>IBM AIX</th>
<th>FreeBSD</th>
<th>Windows</th>
</tr>
</thead>
</table>
| Linux                                 | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• SNMP mode of data collection. default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. Default SNMP port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. Default SNMP port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. Default SNMP port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| Windows                            | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  
| | • Telnet mode of data collection. Default telnet port is 23.  
• SSH mode of data collection. Default SSH port is 22  
• FTP mode of data collection. Default FTP port is 23  
• SNMP mode of data collection. default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.  

### Through WMI API (Windows Management Information ) . RPC Service must be running. (Remote Procedure Call)  
• SNMP mode of data collection, default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.
SNMP Agent Installation
(Adapted from Windows help)

- Installing SNMP Agent on Windows XP/2000/2003
- Installing SNMP Agent on Windows NT
- Installing SNMP Agent on Linux
- Installing SNMP Agent on Solaris

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.

Installing SNMP Agent on Windows XP, 2000 and 2003

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.

1. Click Start, point to Settings, click Control Panel, double-click Add or Remove Programs, and then click Add/Remove Windows Components.
2. In Components, click Management and Monitoring Tools (but do not select or clear its check box), and then click Details.
3. Select the Simple Network Management Protocol check box, and click OK.
4. Click Next.
5. Insert the respective CD or specify the complete path of the location at which the files are stored.
6. SNMP starts automatically after installation.

This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.

Installing SNMP Agent on Windows NT

To install SNMP in Windows NT, follow the steps given below:

1. Right-click the Network Neighborhood icon on the Desktop.
2. Click Properties.
3. Click Services.
4. Click Add. The Select Network Service dialog box appears.
5. In the Network Service list, click SNMP Service, and then click OK.
6. Insert the respective CD or specify the complete path of the location at which the files are stored and click Continue.
7. After the necessary files are copied to your computer, the Microsoft SNMP Properties dialog box appears.

This completes the installation process. To configure SNMP agents respond to SNMP requests, refer to Configuring SNMP agents.
Installing SNMP Agent 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:
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:
   
   1. ./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.
2. make
3. umask 022
4. make install

This completes the installation process. To configure SNMP agents 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:
   1. `./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.
   2. `make`
   3. `umask 022`
   4. `make install`

**Note:** To Install in Solaris 8, Follow the given steps:

5. netsnmp-5.1.1 package is available in the following url
   ```
   ```
   This package is for solaris8 on sparc.
6. gunzip netsnmp-5.1.1-sol8-sparc-local.gz.
7. `pkgadd -d netsnmp-5.1.1-sol8-sparc-local`
   
   The package would be installed. The package is configured with the compile option of " ./configure --with-mib-modules=host ". The agent would have support for host-resource-mib.
8. To start netsnmp agent: Execute - `#/usr/local/sbin/snmpd`
9. To stop this daemon: Execute - `# pkill -9 -x -u 0 snmpd`

This completes the installation process. For configuring SNMP agents to respond to SNMP requests, refer to Configuring SNMP agents.
SNMP Agent Configuration

- Configuring SNMP agent in Windows XP/2000/2003
- Configuring SNMP agent in Windows NT
- Configuring the SNMP Agent in Linux versions prior to 8
- Configuring the SNMP Agent in Linux versions 8 and above
- Configuring the SNMP Agent in Solaris Systems

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, 2000 and 2003 systems, follow the steps given below:

1. Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools** and then double-click **Computer Management**.
2. In the console tree, click **Services and Applications** and then click **Services**.
3. In the details pane, scroll down and click **SNMP Service**.
4. On the **Action** menu, click **Properties**.
5. On the **Security** tab, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.
6. Under Accepted community names, click **Add**.
7. Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.
8. In **Community Name**, type a case-sensitive community name, and then click **Add**.
9. 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 and IP or IPX address, and then click **Add** again.
10. Click **Apply** 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:

1. Click **Start**, point to **Settings**, and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
2. In the details pane, click **SNMP Service** and then click **Properties**.
3. Click the **Security** tab.
4. If you want to send a trap for failed authentications, select the **Send Authentication Trap** check box.
5. Under Accepted Community Names, click **Add**.
6. In the **Community Names** box, type a community name from which you will accept requests.

7. To move the name to the Accepted Community Names list, click **Add**.

8. Repeat step 7 for any additional community name.

9. 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** to move the name to the Only Accept SNMP Packets From These Hosts list.

10. Repeat step 9 for any additional hosts.

11. On the Agent tab, specify the appropriate information (such as comments about the user, location, and services).

12. Click **OK** to apply the changes.

**Configuring the SNMP Agent in Linux versions prior to 8**

For details about installing SNMP agents in Linux systems, refer to [Installing SNMP Agent on Linux Systems](#).

1. Stop the agent if it is running already, using the command: `/etc/rc.d/init.d/snmpd stop`

2. 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.

3. Start the agent using the command `/etc/rc.d/init.d/snmpd start`.

**Configuring the SNMP 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:

1. Insert the line `view allview included .1.3.6` next to the line `# name incl/excl subtree mask(optional)`

2. Change the line `access notConfigGroup "" any noauth exact systemview none none` next to the line `# group context sec.modelsec.level prefix read write notif as` as `access notConfigGroup "" any noauth exact allview none none`
3. Then restart the snmp agent using the following command:

/etc/rc.d/init.d/snmpd restart

**Configuring the SNMP Agent in Solaris Systems**

For details about installing SNMP agents in Solaris systems, refer to [Installing SNMP Agent on Solaris Systems](#).

1. Stop the agent if it is running already using the following command:

   /etc/init.d/init.snmpdx stop

2. Make the following changes in `/etc/init.d/init.snmpdx` file

   a. 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`

   b. Replace the line

   ```
   /usr/bin/pkill -9 -x -u 0 '(snmpdx|snmpv2d|mibiisa)'
   ```

   with

   ```
   /usr/bin/pkill -9 -x -u 0 '(snmpd)'
   ```

3. Restart the agent using the following command:

   `/etc/init.d/init.snmpdx start.`
Security/Firewall Requirements

This section explains how the Applications Manager can be accessed behind a firewall. Fire walls act as barriers preventing unauthorized access to a network. They act as entrance through which authorized people may pass and others not.

You need to configure the firewall so that the host on which Applications Manager runs, can access the monitor at the relevant port.

Ports to be opened when Monitors are behind the firewall:

<table>
<thead>
<tr>
<th>Monitors</th>
<th>Port Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td><strong>WMI Mode of monitoring:</strong>&lt;br&gt;Windows Management Instrumentation (WMI) -- Port: 445&lt;br&gt;Remote Procedure Call (RPC) -- Port: 135</td>
</tr>
<tr>
<td></td>
<td><strong>SNMP Mode of monitoring:</strong>&lt;br&gt;SNMP Agent Port: 161</td>
</tr>
<tr>
<td>Linux / Solaris / AIX / HPUnix</td>
<td>Telnet Port: 23 (if mode of monitoring is Telnet)&lt;br&gt;SSH Port: 22 (if mode of monitoring is SSH)&lt;br&gt;SNMP Agent Port: 161 (if mode of monitoring is SNMP)</td>
</tr>
<tr>
<td>JBoss</td>
<td>Port in which JBoss is running (for eg., 8080) and also, the Hostname should be accessible.</td>
</tr>
<tr>
<td>WebLogic</td>
<td>HTTP Port of WebLogic, for eg., 7001</td>
</tr>
<tr>
<td>Oracle Application Server</td>
<td>HTTP Port of Oracle Application Server, for eg., 7200</td>
</tr>
<tr>
<td>Tomcat</td>
<td>HTTP Port of Tomcat, for eg., 8080</td>
</tr>
<tr>
<td>WebSphere</td>
<td>HTTP Port of WebSphere (default:9080)</td>
</tr>
<tr>
<td>Oracle</td>
<td>HTTP Port of Oracle (default:1521)</td>
</tr>
<tr>
<td>DB2</td>
<td>HTTP Port of DB2 (default: 50000)</td>
</tr>
<tr>
<td>SQL Server</td>
<td>HTTP Port of SQL Server (default:1433)</td>
</tr>
<tr>
<td>MySQL</td>
<td>Port on which MySQL is running eg., 3306</td>
</tr>
<tr>
<td>Mail Server</td>
<td>SMTP Server port: 25 (default), to send mails from Applications Manager</td>
</tr>
<tr>
<td>Exchange Server</td>
<td>HTTP Port of Exchange Server (default:25)</td>
</tr>
<tr>
<td>Web Server - Apache / IIS / PHP</td>
<td>HTTP Port of Web Server (default:80)</td>
</tr>
<tr>
<td>JMX [ MX4J / JDK 1.5]</td>
<td>HTTP Port of JMX agent (default:1099)</td>
</tr>
<tr>
<td>Service Monitoring</td>
<td>HTTP Port of Services (default:9090)</td>
</tr>
<tr>
<td>SNMP</td>
<td>HTTP Port of SNMP (default:161)</td>
</tr>
<tr>
<td>Telnet</td>
<td>HTTP Port of Telnet (default:23)</td>
</tr>
<tr>
<td>Web Transaction</td>
<td>Port in which the agent is deployed (default: 55555)</td>
</tr>
</tbody>
</table>

When there is a two way communication, and the monitors need to access Applications Manager, then the following ports need to be opened.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebServer Port: 9090</td>
<td>Should be opened for accessing the Applications Manager WebClient and also for monitoring WebLogic and JBoss.</td>
</tr>
<tr>
<td>Trap Port: 1620</td>
<td>If Traps are configured to be received in Applications Manager, then you need to open up Trap Port: 1620.</td>
</tr>
</tbody>
</table>

Apart from this, Applications Manager makes sure that data is secure; internal mysql database allows only localhost to access the database through authenticated users. User Names and Passwords are
stored in the MySQL database that is bundled along with the product. The passwords are encrypted to maintain security.

**Privileges required for different monitor types:**

<table>
<thead>
<tr>
<th>Monitors</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Administrator username/password [WMI mode]</td>
</tr>
<tr>
<td>Linux</td>
<td>Guest user privilege</td>
</tr>
<tr>
<td>Solaris</td>
<td>Guest user privilege</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>Guest user privilege is sufficient but for collecting Memory related details, a user with &quot;root&quot; privilege is required. Hence, it is preferable to use a &quot;root&quot; account to view all details</td>
</tr>
<tr>
<td>HP Unix</td>
<td>Guest user privilege</td>
</tr>
<tr>
<td>MS SQL</td>
<td>System Administrator/Owner for the &quot;master&quot; database</td>
</tr>
<tr>
<td>MySQL</td>
<td>User name specified should have access to the databases that are to be monitored. MySQL should also be configured to allow the host on which App Manager is running to access the MySQL database.</td>
</tr>
<tr>
<td>DB2</td>
<td>Permission of &quot;sysproc procedure&quot; user of the DB2 database</td>
</tr>
<tr>
<td>Oracle</td>
<td>Permission of &quot;system&quot; user of the Oracle database</td>
</tr>
<tr>
<td>WebSphere</td>
<td>If Global Security is enabled, the username/password for the same. Else no username/password is required.</td>
</tr>
<tr>
<td>WebLogic</td>
<td>If WebLogic is authenticated, the username/password for the same. Else no username/password is required.</td>
</tr>
<tr>
<td>JBoss</td>
<td>If JBoss is authenticated, the username/password for the same. Else no username/password is required</td>
</tr>
<tr>
<td>Tomcat</td>
<td>If 5.x, you need to have username and password to connect to Tomcat Manager Application. Else no username/password is required. The user specified should have 'manager' role.</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>SNMP Community string with read privileges</td>
</tr>
</tbody>
</table>