



User Guide

Technical Support

appmanager-support@manageengine.com

Website

<http://www.manageengine.com/apm>

© 2012 Zoho Corp. All Rights Reserved

Table of Contents

INTRODUCTION.....	8
Key Features	9
Monitoring Capabilities.....	12
What's New in Release 10.3	15
INSTALLATION AND SETUP	26
System Requirements.....	27
Differences between Windows and Linux versions of Applications Manager.....	29
Installing and Uninstalling	30
Licensing Applications Manager	36
Using Update Manager	37
Starting and Shutting Down Applications Manager	38
GETTING STARTED	40
Understanding Applications Manager	41
Prerequisites for Applications Manager.....	45
Working with Applications Manager	57
WORKING WITH MONITOR GROUPS	58
Creating Monitor Groups.....	59
Creating New Web Application Group.....	61
VMware Virtual Infrastructure Groups	63
Associating Monitors to Monitor Groups.....	64
Deleting Monitor from Monitor Groups	65
Editing and Deleting a Monitor Group	66
CONFIGURING NEW MONITOR.....	67
Application Servers	69
Database Servers	81
Middleware / Portal	87
Services.....	90
Mail Servers.....	96
Web Server / Services	98
Servers	104
HTTP URL Monitors.....	107
Oracle E-Business Suite	112
SAP Server Monitors	113
SAP CCMS Monitors	114

Virtualization	115
VMware ESX/ESXi Servers	116
Microsoft Hyper-V Servers add-on	117
Amazon Monitors	118
Custom Monitors	119
File / Directory Monitor	120
Windows Performance Counters	121
Script Monitors	122
Database Query Monitor	125
J2EE Web Transaction Monitor	126
Java Runtime Monitor	127
Custom Monitor Type	128
VIEWING PERFORMANCE METRICS	131
Application Servers	134
Microsoft .NET	135
GlassFish Servers	137
JBoss Servers	139
Oracle Application Servers	142
SilverStream Servers	145
Tomcat Servers	147
WebLogic Servers	149
WebSphere Servers	153
Database Servers	156
Oracle DB Servers	161
MS SQL DB Servers	169
IBM DB2 DB Servers	174
Sybase DB Servers	178
PostgreSQL DB Servers	181
Memcached Servers	185
Middleware / Portal	187
Microsoft MQ (MSMQ)	188
Microsoft Office Sharepoint Servers	190
WebLogic Integration Servers	195
IBM WebSphere MQ	197
VMware vFabric RabbitMQ	199
Servers	202
Windows Servers	209
Configuration	214
Linux Servers	216
IBM AS400 / iSeries	221

Virtualization	234
VMware ESX/ESXi Servers	235
Virtual Machines.....	240
Microsoft Hyper-V Servers.....	244
Hyper-V Virtual Machines	251
Cloud Apps	253
Amazon.....	254
Amazon EC2 Instances.....	258
Amazon RDS Instances	262
Services.....	265
Mail Servers	272
Web Server / Services	277
Real Browser Monitor	281
HTTP URL Monitors.....	285
Oracle E-Business Suite Monitor	287
SAP Server Monitors	289
SAP CCMS Monitors	294
Custom Monitors.....	296
Adding JMX MBeans Attributes	297
Adding SNMP OID Attributes.....	299
File / Directory Monitor.....	300
WINDOWS PERFORMANCE COUNTERS	301
Script Monitors	302
Java Runtime Monitor	306
Database Query Monitor.....	312
J2EE Web Transaction Monitors.....	314
J2EE Web Transaction Agent.....	315
J2EE Web Transaction Metrics	317
ManageEngine OpManager Network Monitoring Connector	319
ManageEngine OpStor SAN Monitoring Connector	321
ALARMS.....	323
Alarm Details	325
Viewing and Configuring Alarms Globally	327
Creating Threshold Profile	328
Creating Actions	329
Sending E-mail.....	330
Sending SMS	331
Sending Trap	334
Execute MBean Operation.....	336
Log a Ticket	338

Perform Java Action.....	339
Perform Amazon EC2 Instance Action	340
Perform Virtual Machine Action	341
Windows Services Action	342
Replaceable Tags	343
Associating Threshold and Action with Attributes	345
Alarm Escalation	346
Bulk Alarm Configuration	347
Configuring Dependencies and Alarm Rules.....	348
Configuring Consecutive Polls	351
VIEWING REPORTS	352
Grouping of Reports	354
7 / 30 Reports	366
ADMIN ACTIVITIES.....	371
Discovery and Data Collection	373
Bulk Import of Monitors	374
Discovery	377
Custom Monitor Type.....	379
Performance Polling.....	382
Downtime Scheduler.....	384
Server Process Templates	385
Windows Service Templates	386
Alarm/Action	387
Availability Settings	388
Action / Alarm Settings.....	390
Windows Event Log Rules	392
Alarm Escalation	393
Configure Global SNMP Trap	394
SNMP Trap Listener	395
Applications Manager Server Settings	397
Global Settings.....	398
Configure Mail Server	400
Configure SMS Server	401
Configure Proxy	402
User Administration.....	403
Add-On/Product Settings	407
Logging	409
Personalize Web Client.....	410
Integration with Portals	411
REST API.....	412
JSON Feed	413

Dashboards.....	414
World Map Business View	415
Reporting	416
Reports Settings	417
Enable Reports	419
Schedule Reports	420
Business Hours	421
Upload Files/Binaries	422
Bulk Configuration of Monitors	423
Data Backup	425
Server Settings	426
Production Environment.....	428
REST APIS	430
List Monitor API	433
List Server API.....	435
List Alarms API	437
Manage API.....	440
Authenticator API.....	442
ExecuteAction.....	444
ListDashboards API	445
ListMonitorTypes API.....	447
ListMonitorGroups API.....	450
ListMGDetails API.....	454
ListMGDetails API.....	461
ListMGDetails API.....	468
ListMGDetails API.....	475
ListMGDetails API.....	482
ListMGDetails API.....	489
ListActions API.....	496
Search API	498
ShowPolledData API.....	501
Ping API.....	504
MaintenanceTask	506
CreateMaintenanceTask API	507
EditMaintenanceTask API.....	510
DeleteMaintenanceTask API	513
GetMaintenanceTaskDetails/ListMaintenanceTaskDetails API	514
GetMonitorData API.....	515
AddMonitor	516
AddMonitor API - Application Servers	518
AddMonitor API - ERP	525

AddMonitor API - Java/Transaction	527
AddMonitor API - Servers	529
AddMonitor API - Database Servers.....	537
AddMonitor API - Services.....	543
AddMonitor API - Web Server/Services.....	551
AddMonitor API - Mail Servers	555
AddMonitor API - Middleware/Portal.....	557
AddMonitor API - Custom Monitors	560
AddMonitor API - Virtualization	562
AddMonitor API - Cloud Apps.....	564
AddMonitor API - EUM Monitors.....	565
ListUserDetails API	571
PolINow API.....	573
DeleteMonitor API.....	574
Error Handling.....	575
END USER MONITORING (EUM)	580
How does End User Monitoring (EUM) Work?	581
Installing and Uninstalling EUM Agent	583
EUM Dashboard	586
APM INSIGHT - AN OVERVIEW	587
How does APM Insight work?	588
Installing the APM Insight Agent	589
APM Insight Agent Configuration Options.....	596
APM Insight Dashboard	601
Web Transaction.....	602
Apdex Score	604
ENTERPRISE EDITION.....	605
Enterprise Edition - Admin Server	607
Enterprise Edition - Managed Server	610
Enterprise Edition - Failover Support	611
ANOMALY DETECTION	615
SLA MANAGEMENT CONSOLE FOR MANAGERS	620
TECHNICAL SUPPORT & PRODUCT INFORMATION.....	622
GLOSSARY	626
PRODUCT FAQ.....	629
WEB CLIENT	630
Icon Representation.....	632
Custom Dashboards	635
Custom Fields.....	639
Mobile Web Client.....	641

APPENDIX.....	643
Applications Manager Home	644
Data Collection - Host Resource	645
SNMP Agent Installation	646
SNMP Agent Configuration	650
Security/Firewall Requirements	654
User Management Security Policy	658
Forums / Blogs.....	660
Add-Ons	662
TROUBLESHOOTING.....	663
HOW TO DEMOS	664
BEST PRACTICES	665

Introduction

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

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

Alarms 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 alarms, 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.

Note: By clicking on the *Help link* in the Web Client, you can access the **context sensitive help pages**.



Key Features

The following are some of the key features of Applications Manager.

Note: Apart from the below-mentioned applications, you can also monitor your own custom applications via scripts. It will be added as a New Monitor Type.

Feature	Description
Application Server Monitoring	Monitors Microsoft .NET, SilverStream, GlassFish, WebLogic, WebSphere, Tomcat, VMware vFabric tc Server, Oracle Application Server, JBoss Application Server and also web-based applications such as Servlets, JSP, and EJB of the application servers.
Middleware / Portal Monitoring	Monitors WebLogic Integration, IBM WebSphere MQ, Microsoft Office Sharepoint, and Microsoft Message Queue (MSMQ) servers.
SAP Monitoring	Monitors the performance of SAP Servers and SAP CCMS servers.
Oracle EBS Monitoring	Monitors the modules of Oracle E-Business Suite
Web Transactions Monitoring	Monitor J2EE Web Transactions end to end, with performance metrics of all components starting from URLs to SQLs.
Virtualization Monitoring	Monitor VMware ESX/ESXi servers, Microsoft Hyper-V servers and their guest virtual machine instances. Support for monitoring virtual infrastructure components such as data center and cluster through vCenter.
Cloud Apps Monitoring	Support for monitoring Amazon EC2 & RDS instances, attached EBS volumes and Amazon S3 buckets.
Database Monitoring	Supports monitoring of MySQL, Oracle, IBM DB2, Sybase, MS SQL, PostgreSQL and Memcached servers.
Host Resource Monitoring	Monitors the performance of Windows, Linux, Solaris, HP Unix, Tru64, Mac OS, Unix, IBM AIX, IBM AS400 / iSeries, Novell and FreeBSD servers. Also monitors Event Logs for Windows.
Java Runtime Monitor	Provides out-of-the-box remote monitoring and management on the Java platform and of applications that run on it.
File System Monitor	Monitors changes in the selected files and directories.
Windows Performance Counters	Monitors windows performance counter values through WMI.

Feature	Description
Ping Monitor	Checks for availability of a device, server or network device.
Script Monitoring	Ad-hoc Windows/Linux custom scripts, used in-house can be managed from the same web console. Additionally, QEngine, a test automation suite has been integrated in Applications Manager.
Services Monitoring	Monitors Services such as FTP, DNS, SFTP, Telnet, RMI adaptor, TCP port, etc.
Mail Servers Monitoring	Monitors Mail servers (including SMTP servers and POP servers) and Microsoft Exchange Server.
WebServices Monitoring	Monitors Apache, IIS,PHP,SSL Certificate,Web Services (SOAP) and other web servers.
End User Experience Monitoring	Provides the ability to measure the experience of your end users. Includes support for Real Browser Monitor, DNS, Ping, LDAP and Mail Server monitors.
HTTP URL Monitoring	Monitors any HTTP or HTTPS -based URL of web pages.
Custom Application Management	Groups data sources from multiple resources and displays them in a common place. The data sources can be JMX MBeans and SNMP agents.
Fault Management	Sends ' <i>Alarms</i> ' based on the monitored attributes. These can be escalated through e-mail / SMS /trap/ MBean Operation/ execute a program.
Performance Reports	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.
Intuitive Web Client	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.
Holistic view to Monitor Group	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.

Feature	Description
Graphical Representation of Attribute Statistics	The attribute details are represented through graphs that provides an easy approach to understand the " attribute vs time " statistics for one hour. Also the icons  and  provided in the graphs represent details about the statistics for 7 days and 30 days respectively.
Scalable Architecture	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.
Root Cause Analysis	Provides details on the different severity levels by identifying its reason/cause.
Business Service Management	Helps the Manager to have an integrated high-level view of the Business Infrastructure. Location intelligence is added via World Map Business View.

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.

Note: Apart from the applications mentioned below, you can monitor your own custom applications via scripts. It will be added as a new monitor type.

1. Application Servers
 - GlassFish Servers
 - JBoss Servers
 - Microsoft .NET
 - Oracle Application Servers
 - SilverStream
 - Tomcat Servers
 - VMware vFabric tc Server
 - WebLogic Servers
 - WebSphere Servers
2. Database Servers
 - IBM DB2 Database Servers
 - Memcached Database Servers
 - MS SQL Database Servers
 - MySQL Database Servers
 - Oracle Database Servers
 - PostgreSQL Database Servers
 - Sybase Database Servers
3. Middleware / Portal
 - IBM WebSphere MQ
 - Microsoft Message Queue (MSMQ)
 - Microsoft Office SharePoint
 - WebLogic Integration Servers
 - VMware vFabric RabbitMQ

4. ERP

- Oracle E-Business Suite
- SAP CCMS Server
- SAP Server

5. Virtualization Solutions

- Hyper-V servers
- Virtual Machines
- VMware ESX/ESXi servers

6. Cloud Apps

- Amazon EC2
- Amazon RDS
- Amazon S3

7. Services

- Active Directory
- DNS Monitor
- FTP / SFTP Monitor
- JMX Applications
- LDAP Monitor
- Ping Monitor
- Service Monitoring
- SNMP
- Telnet

8. Mail Servers

- Mail Server
- Microsoft Exchange Server

9. Web Server / Services

- Apache Server
- HTTP(s) URL Monitors and HTTP(s) URL Sequence (Record & Palyback)
- IIS Server
- PHP
- Real Browser Monitor
- SSL Certificate Monitor

- Web Server
- Web Services

10. Servers

- Free BSD
- HP Unix / Tru64 Unix
- IBM AIX
- IBM AS400 / iSeries
- Linux
- Mac OS
- Novell
- Solaris
- Windows

11. Custom Monitors

- Database Query Monitor
- File System Monitor
- JMX / SNMP Dashboard
- Script Monitor
- Windows Performance Counters

12. Java / Transaction Monitors

- J2EE Web Transactions Monitor
- Java Runtime

What's New in Release 10.3

- Out-of-the-box support for monitoring the performance and availability of **VMware vFabric RabbitMQ** messaging systems.
- Web client user authentication using LDAP/AD.
- Web client GUI enhancements.
- Customizing the logo in reports.
- Support for embedding different world map views.
- Support for monitoring SSLv3 enabled websites in URL monitoring.

What's New in Release 10.2

- Support for monitoring Oracle JRockit JVM in Java Runtime Monitor.
- Support for monitoring IBM JVM in Java Runtime Monitor.
- Ability to play sound for critical alarms.
- Performance Metric Widget enhanced to show graphs for additional metrics with scaling option.

What's New in Release 10.1

- Out-of-the-box support for monitoring the availability and performance of **VMware vFabric tc servers** and the Spring Applications deployed on the server.
- We now support monitoring of validity and expiry dates of SSL Certificates.
- Support for Gmail in Mail Server Configuration.
- Ability to add new Event Logs other than the available default ones.
- Support for monitoring SOAP Operations with headers.

What's New in Release 10.0

- End User Experience Monitoring (EUM) add on introduced. The 'Real Browser Monitor' add-on has been rechristened as 'End User Monitoring' add-on with enhancements that help it go beyond real browser monitoring. This now includes LDAP, DNS, Ping and Mail Server RTT. Also, the pricing structure of RBM has been modified from an agent-based model to a flat-fee model.
- Custom fields and labels for monitors and groups. You can view this by clicking on the 'Custom Fields' button inside a monitor or monitor group.
- We now show split up of CPU utilization by CPU cores. There is also support for viewing server configuration parameters.
- Improved web client and ability to customize tabs.

- Support for monitoring Virtual Infrastructure through vCenter server.
- Support for Amazon S3 monitoring.
- Ability to specify roles for Exchange server 2007/2010. This helps view more performance metrics.
- A 64-bit binary for Applications Manager.
- IPV6 support for most monitor types.
- Anomaly Detection is no more an add-on feature. It will be part of the basic product.
- SSL support for SMTP and POP in mail server monitor.

What's New in Release 9.5

- Ability to automatically provision virtual resources based on threshold breaches. You can create actions to automatically start, stop and restart VMs of both VMware ESX and Hyper-V servers from Applications Manager.
- Ability to automatically provision cloud resources based on threshold breaches. You can create actions to automatically start, stop and restart Amazon EC2 instances from Applications Manager.
- Out-of-the-box support for monitoring the availability and performance of Microsoft Message Queue (MSMQ)
- Option to associate multiple dependent devices across managed servers.
- Enhancements to fault management module including the option to execute email/SMS actions during selected business hours and the option to execute actions for a specific number of times or repeatedly until it gets acknowledged.

What's New in Release 9.4

- Out-of-the-box support for monitoring the availability and performance of **Microsoft Hyper-V servers** and their guest virtual machines. Applications Manager now supports multiple virtualization vendors such as VMware and Microsoft.
- Introduced server process templates/Windows service templates which are a pre-defined, reusable collection of processes. They provide an easy way to add multiple server processes/templates for monitoring across a group of servers.
- Improved method of managing operations in web services. Includes the ability to specify SOAP Action and Request values corresponding to the operation and also the ability to add custom operations.
- New REST APIs to add different monitor types, delete and list monitors.
- Options to stop, start and reboot Amazon EC2 instances from within Applications Manager.
- Additional performance metrics for MySQL DB servers including information about system variables of the MySQL server.

What's New in Release 9.3

- Out-of-the-box support for monitoring the availability and performance of **Amazon EC2 and RDS instances**. Applications Manager helps you ensure your business-critical cloud-based applications and services are performing well at all times.
- Introduced new report type for monitor groups known as **Availability and Downtime Trend Report**. This report compares the availability of the monitor group against target availability and also shows the downtime count and total downtime for the monitor group.
- Enhancements to SNMP Trap listener feature including the ability to select trap severity based on threshold profiles.
- Support for monitoring Exchange server 2010.
- Option to monitor WebSphere Application Server through secure SSL mode.
- Support for associating dependent devices across managed servers in the Enterprise edition. This will help you better organize your monitors and reduce redundant checks.

What's New in Release 9.2

- Out-of-the-box support for monitoring the availability and performance of **VMware ESX/ESXi** host servers and their guest virtual machine instances. Applications Manager provides a single console for monitoring both physical and virtual components of a heterogeneous IT environment.
- Comprehensive monitoring of **Memcached servers** to help you detect and diagnose problems with your caching systems faster.
- Support for monitoring **PostgreSQL** database servers.
- Introduced **Web application group** which is a new type of Monitor Group. This will be useful for grouping your web infrastructure into logical components such as servers, databases, web servers, etc and better manage the relationship between components.
- An improved **Real Browser Monitor (RBM) dashboard** that provides an overview of the status of your web transactions from multiple locations.
- New REST APIs to create, edit and delete downtime schedulers, get monitor data, and add monitors.
- Option to send events as SNMP Traps to external SNMP Trap listeners.
- Enhancements to Java Runtime Monitor including the ability to know how garbage collection behaves in the JVM. You can also see the impact of the GC on thread dump with history and view historical JVM configuration parameters.
- Support for monitoring Windows 7 server.
- Support for monitoring WebSphere Application Server version 7.
- Issues fixed include ServiceDesk Plus integration issue when customers enable AD authentication in ServiceDesk Plus. | [More](#)

What's New in Release 9.1

- New monitor type called "Real Browser Monitor" (RBM) introduced. RBM opens up a Microsoft Internet Explorer browser and monitors a web application just like how a real user sees it. It supports playback from different geographical locations.
- Get notified of anomalies in a production application by defining anomaly profiles on performance metrics. Support for anomalies based on fixed baseline, moving baseline and custom expressions. There is also an Anomaly Dashboard introduced to facilitate viewing all the performance metrics.
- REST APIs introduced to make integration of Applications Manager with internal portals and other monitoring tools easier.
- At a glance Report that provide a summary of Top 10 monitors based on various performance metrics and uptime. You can view reports by Monitors, Monitor Types and Monitor Groups.
- Alarm Management : Define dependent device for a Monitor Group or individual monitor to suppress false downtime alarms caused by the dependent device being down.Enhanced alarm configuration rules for health and availability of Monitor Group.
- Monitor Group Template Dashboards have been introduced. This will help configure a custom dashboard and reuse it for multiple Monitor Groups (business applications or customers) - based on how you use the product.
- New widgets called "Bookmarks" and "Custom Text and HTML" for Integrating knowledge base articles and other web links added to Custom Dashboards.
- To enhance Web Client security, configurable Account policies has been added to the User Administration Module.

What's New in Release 9

- Microsoft SQL Server database back-end support.
- Support for monitoring Oracle E-Business Suite.
- Ability to create custom dashboards.
- Enhancements in server monitoring.
- Enhancements in WebClient look and feel.
- The MySQL DB Server bundled in the product has been upgraded from version 4.0.13 to version 5.0.52.

What's New in Release 8.6

- Monitor the performance of AS400 / iSeries.
- Support for monitoring SAP CCMS metrics.
- LDAP, DNS and FTP/SFTP Service Monitors are now supported by Applications Manager.

- Additional metrics such as Hour of day, Day of week, Statistical and Heat chart report tabs in 7,30 History data are added.
- Support for Monitor Group/Sub-Group in downtime scheduler.
- Ability to assign Sub-Group for operator role.

Issues Fixed in 8.6

- Issue in Database Query monitor is fixed. It now retains only new data collected across all rows and columns.
- Memory leak issue in JBoss monitoring is fixed.
- Issue fixed in infinite loop in URL monitors.
- Issue in associating monitors to a monitor group with same name is fixed. | More...

What's New in Release 8.5

- Database Query Monitor is now supported by Applications Manager.
- Applications Manager now supports Active Directory Monitoring.
- A new flash-based graphical view, called Business View, is added to view IT infrastructure.
- Support for database details in MySql monitors that are collected once per day based on configuration is added.

Issues Fixed in 8.5

- Issue in Configure Alarms for Script and Query monitor when scalar attributes are not available is fixed.
- Issue in collecting Performance metrics for Weblogic 9 and 10 datacollection, when WLS server is restarted without restarting Applications Manager, is fixed.
- Issue fixed in Server Monitors when memory load increases leading to Out Of Memory.
- Issue fixed to have multiple network interface on the same host. | More...

What's New in Release 8.4

- ManageEngine Applications Manager integrates now with a comprehensive Network Monitoring Tool, ManageEngine OpManager.
- In WebServices monitoring, added support for generating alarms based on the output of the service.
- Free Edition of Applications Manager will not support DB2, Sybase in addition to Add-ons.
- J2EE Web Transactions, IBM WebSphere MQ Series and MS Office Sharepoint have been modified as Add-ons.

Issues Fixed in 8.4

- Issue in synching of data between the Managed Servers and Admin Servers is fixed.
- Issue in showing the status in Icons View and Table view is fixed

- Fixed issue in enabling and disabling SSL in AMServer.properties is fixed Cleanup entries are added for the Script Table data
- Fixed issue in Archiving for Tomcat Session and Oracle Users. | More...

What's New in Release 8.3

- IBM WebSphere MQ, SilverStream, Microsoft Office Sharepoint Server, GlassFish Server Monitor Support added
- Windows Vista monitoring support added
- Oracle 10.1.3 monitoring support added
- Support for Custom attribute reports added
- Poll Now - option added for monitors
- Restricted access of Monitor Groups for Managers.

Issues Fixed in 8.3

- Fixed issue in Google Map display when the monitor group display name contains single quotes.
- While creating the Monitor Group (MG), the owners select box is shown empty when the latest MySQL Driver is used.
- In MySQL monitoring, when the '**last error**' attribute is having special characters the polling will stop for that monitor.
- The performance issue in deleting the NA rows in script monitor is fixed. | More...

What's New in Release 8.2

- Availability and Health Reports - Critical Snapshot, History reports added
- Availability Trend Report, Outage Comparison Report added
- Ability to configure Business hours for reports added
- Support for bulk import of monitor configurations
- Support for sending SMS alarms via Modem
- Network Interface monitoring in WMI mode added

What's New in Release 8.1

- Sybase Support added
- Outage Comparison Reports, Availability Trend Reports, Availability and Health Snapshot Reports added
- Support for adding custom monitor types
- MySQL monitoring enhancements added
- Network Interface monitoring added

What's New in Release 8

- SAP Server Monitoring support added
- Enhancements in Availability and Performance Dashboards
- DB2 Monitoring Enhanced
- Improvement in scalability of reports
- WebClient Enhancements

What's New in Release 7.4

- Ping Monitor support added
- Support for Secondary Mail Server configuration
- Support for creating a Monitor Group within a Monitor Group (Monitor Sub-Group)
- Support for Monitor Group creation in Admin Server (Enterprise-Edition Setup)
- Ability to treat Monitor Group as a Services Group or as an Application Cluster has been added.

What's New in Release 7.3

- Localized webclient to support German, Spanish and French languages
- Support for monitoring Windows Performance Counters in Windows 2000
- Availability and Health realtime snapshot report for Monitor Groups added
- Support for JSON Feeds for integrating Applications Manager data in corporate intranet
- \$DATE tag enhancements in actions.
- Alarm Escalation added

What's New in Release 7.2

- WebLogic Integration Server Monitoring
- Support for Java Runtime Monitor
- File System Monitoring
- Failover support for Enterprise Edition
- IIS Enhancements
- WebSphere Enhancements
- Script Monitoring Enhancements - Table support added
- WebClient Enhancements

What's New in Release 7.1

- Web Services (SOAP) Monitoring
- Windows Performance Counters Monitoring

- Support for monitoring Mac OS
- JBoss 4.0.4 Support
- WebLogic 9.2 Support
- Ability to specify the attribute type for JMX and SNMP Monitors
- Windows Authentication Support for MS SQL Server monitoring
- New Plasma View of monitors added
- Ability to compare reports is added
- Customizable UI for home tab and Plasma View
- Bulk update of Poll intervals added
- More \$Tags support in executing actions (\$OID, \$DATE, \$URL)
- SSH Key based authentication for Remote Script Monitoring and Execute Program Action
- Ability to set auto refresh time interval added.
- New *Simple* web client layout added. Option to choose between Classic and Simple layouts.
- New Maroon color theme added for personalizing the webclient
- While creating new monitors, troubleshooting is made easy via *Diagnose* Link

What's New in Release 7

What's New in Update for 7

- Remote sessions opened in Server monitoring, issue fixed
- Script Monitoring issues fixed
- Issue in invoking MBean Operation in JMX 1.2 fixed

What's New in Release 7

- Enterprise Edition - Support for large scale monitoring with a distributed setup
- Support for Windows Services monitoring
- Support for Remote Script monitoring
- Server Monitoring Enhancements (HP-UX, IBM AIX, Linux, Solaris)
- Webclient and Server Performance Enhancements
- Webclient HTTPS support
- Improved Fault Management capabilities
- Support for Authenticated JMX Agents
- Improved multi-lingual support
- Other bug fixes and minor enhancements

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 alarm 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 alarms 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.
- Alarm Enhancements like Pick/Unpick alarms, Annotation of alarms have been provided.
- Polls to retry can be configured individually for any attribute of a Monitor.
- Multiple varbind support in alarm 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.
- Alarm Template feature for bulk alarm 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
- Windows vs Linux Downloads
- Installing and Uninstalling
- Licensing
- Using Update Manager
- Starting and Shutting Down
- Troubleshooting

System Requirements

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

Hardware

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

Up to 250 monitors (with medium load on the monitored servers)

Operating Platform	Processor Speed	Memory	Hard Disk Space Required
Windows/Linux	1.4 GHz	2 GB RAM	20 GB

250 - 1000 monitors - Enterprise Edition Setup (One Admin & 2-3 Managed Servers)

Per Managed Server/Admin Server

Operating Platform	Processor Speed	Memory	Hard Disk Space Required
Windows / Linux	1.8 GHz	2 GB RAM	40 GB

1000 monitors and above - Enterprise Edition Setup (One Admin & 4 Managed Servers and above)

Per Managed Server/Admin Server

Operating Platform	Processor Speed	Memory	Hard Disk Space Required
Windows / Linux	Dual processor 1.8 * 2 GHz	2 GB RAM - Managed Server	100 GB or higher based on monitors

* If number of Managed Servers are high, 4 GB RAM for the Admin Server is recommended.

Note: It is recommended to read the Best Practices Guide before going into production.

Real Browser Monitor System requirement (for the machine where RBM Agent is to be deployed):

RBM Agents have to be installed on a dedicated Windows Machine - 256 MB RAM, 1 GB HD with Internet Explorer 6 or above. However, Applications Manager can be installed on Windows or Linux. This works with the Professional Edition and Enterprise Edition (with Managed Server). Know more about Real Browser Monitor.

Software Requirements

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

Supported Operating Systems

- Windows Professional / XP / 2000 / 2003 /2008 / Vista / Win 7
- RedHat Linux 8.0 and above
- Enterprise Linux 2.1 and above / Debian / Suse / Ubuntu / Mandriva / CentOS / Fedora Core

Note: Do take a look at the **Windows Vs Linux Downloads** page. Compare the capabilities of Windows and linux variations before proceeding to download the product.

Supported Browsers

- Internet Explorer 6.0 and above
- Firefox 2.x and above

Differences between Windows and Linux versions of Applications Manager

Although most of the Applications Manager features are supported on both the Windows and Linux versions, there are certain features which are only available in the Windows version.

Features supported only in the Windows Version:

The Microsoft applications/servers listed below can be monitored only using the Windows version of Applications Manager. This is because the data collection happens through WMI (Windows Management Instrumentation):

- Exchange Server
- Active Directory
- Microsoft .Net
- Hyper-V
- MSMQ
- SharePoint
- IIS Server
- Windows Performance Counters(any parameter related to Win32_PerfFormattedData)

Apart from these monitors, other features that are supported only in the Windows version are:

Event log rules: Any event can be monitored and notified when it occurs. This is useful when any application generates a failure event in the Windows Event log viewer. This is helpful in a way that the event log comes before the application actually crashes. This serves as a proactive mode of monitoring your applications and services.

NTLM authenticated URLs and Recording HTTP(s) Sequence/Real Browser Monitor(RBM): You can record the HTTP(s) sequence through Recorder.exe tool which works only from a Windows OS. However, you will be able to save the sequence to Applications Manager on a Linux OS.

NOTE: In the Linux Version of Applications Manager, Windows Server Monitoring is possible only in the **SNMP mode**.

Installing and Uninstalling

The following are the Applications Manager product Installations.

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

Free Edition: This allows you to monitor **Five** monitors (This excludes the Monitors added by default). The Free Edition never expires and you get most of the functionality of Professional Edition. See the difference between Free Edition and Professional Edition.

Professional / Enterprise Edition (Trial): You can avail 30 days of evaluation with no restrictions on number of monitors. Professional Edition allows you to monitor up to 250 monitors. Enterprise Edition allows you to monitor more number of servers and applications in a distributed setup. You can configure independent Applications Manager installations to monitor resources and then collectively view the data of all the independent Applications Manager installations ("Managed Server") from a single central installation ("Admin Server").

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

To know the comprehensive difference between Professional and Enterprise Edition features, visit our website - [Feature Comparision](#).

Note: You can upgrade the Professional Edition / Enterprise Edition Trial and Free Edition to **Professional / Enterprise Registered Edition**. This is applicable, if you have purchased ManageEngine Applications Manager and hold the registered license key. To upgrade your license, refer [Licensing Applications Manager](#).

- To install Applications Manager in Windows (.exe)
- To install Applications Manager in Linux (.bin)
- Troubleshooting Installation
- Uninstalling Applications Manager

To Install Applications Manager in Windows (.exe)

1. Download and Execute the 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, Japanese, Vietnamese, French, German, European Spanish, Korean, Hungarian and Traditional Chinese.
4. The next screen prompts for the product edition (**Free Edition, Professional Edition, Enterprise Edition**). Select the preferred edition to install. If **Professional** - is selected, follow the below given steps.
5. Provide the location where the Applications Manager should be installed in your machine. Click **Browse** to provide a different location of installation. Click **Next**.
6. Specify the name of the Folder to be placed in Program Folder. The default is **ManageEngine Applications Manager 9**. Click **Next**.
7. 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
8. Select the Database back-end support - MySQL (Bundled with the product. No Setup required) or Microsoft SQL Server (version 2005 and 2008).
9. If you select Microsoft SQL Server, you need to select if it is based on **SQL Authentication** or **Windows Authentication**. If it is based on SQL Authentication, enter the Host Name, Port Number, Database Name, User Name, Password of the SQL Server. If it is based on Windows Authentication, enter the Host Name, Port Number, Database Name of the SQL Server and the User Name , Password of the machine in which SQL Server is running. Also provide minimum privileges required : The user account should be the DB_Owner of the created Database.
10. 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. 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. [More Information on 'Manually Installing Applications Manager as Service'].]

11. Current Settings is displayed in the next screen. If you need to make changes, click **Back**, else click **Next** to continue installation.
12. If you had earlier selected **Professional Edition**, now you have to choose whether it is **trial** or **registered**. If registered, the next screen will prompt you to select the registered license file from your system.
13. If you had selected **Free License**, follow the steps from 5to 9 .
14. If you had selected **Enterprise Edition**, choose if you want install applications manager as **Admin Server** or **Managed Server**.
15. If you had selected **Enterprise Edition - Admin Server**, next you have to enter the Admin server host name, Port number and SSL Port number. Then, follow the steps from 5 to 9.

16. If you had selected **Enterprise Edition - Managed Server**, enter the associated admin server Host name and SSL port number. If a proxy server is needed to contact the admin server from the Managed Server machine, Enter the Host name, Port number, username and password of the proxy server.
Then follow steps from 5 to 9.
17. You have an option to fill up a **registration form** for Technical Support.
18. Finally, you would be given two options - 1. To view the **ReadMe** file 2. To **launch Applications Manager** immediately.
19. 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. Read the license agreement and click **Next**.
3. The next screen prompts for the product edition (**Free Edition, Professional Edition, Enterprise Edition**). Select the preferred edition to install. If **Professional** - is selected, follow the below given steps.
4. Select the **language** in which you wish to install Applications Manager. The options are English, Simplified Chinese, Japanese, Vietnamese, French, German, European Spanish, Korean, Hungarian and Traditional Chinese.
5. Choose whether it is **trial** or **registered**. If registered, the next screen will prompt you to select the registered license file from your system.
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. Select the Database back-end support - MySQL (Bundled with the product. No Setup required) or Microsoft SQL Server (version 2005 and 2008).
8. If you select Microsoft SQL Server, you need to select if it is based on **SQL Authentication** or **Windows Authentication**. If it is based on SQL Authentication, enter the Host Name, Port Number, Database Name, User Name, Password of the SQL Server. If it is based on Windows Authentication, enter the Host Name, Port Number, Database Name of the SQL Server and the User Name , Password of the machine in which SQL Server is running. Also provide minimum privileges required : The user account should be the DB_Owner of the created Database.
9. Provide the **location** where the Applications Manager should be installed in your machine. Click **Next**.
10. Current Settings is displayed in the next screen. If you need to make changes, click **Back**, else click **Next** to continue installation.
11. Click **Finish** to complete the installation process.
12. If you had selected **Free License**, follow the steps from 4 to 9 .

13. If you had selected **Enterprise Edition**, choose if you want install applications manager as **Admin server** or **Managed server**.
14. If you had selected **Enterprise Edition - Admin Server**, next you have to enter the Admin server host name, Port number and SSL Port number. Then follow the steps from 4 to 9.
15. If you had selected **Enterprise Edition - Managed Server**, enter the associated Admin server Host name and SSL port number. If a proxy server is needed to contact the admin server from the Managed Server machine, click on the proxy server check box. In the next screen, enter the Host name, Port number, User Name and Password of the proxy server. Then follow steps from 4 to 9.
16. You have an option to fill up a **registration form** for Technical Support.
17. Finally, select if you want to view the **ReadMe** file or click **Finish** to launch Applications Manager immediately.

Note: You can install Applications Manager via **Command Line** also. If the file name is **ManageEngine_ApplicationsManager_9_linux.bin**, then type the following command in the command prompt:

```
./ManageEngine_ApplicationsManager_9_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_9_linux.bin**, create a text file named **ManageEngine_ApplicationsManager_9_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 appmanager-support@manageengine.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

[for Windows] - **<File Name>.exe -is:tempdir \$DIRNAME**

[for Linux] - **./<File Name>.bin -is:tempdir \$DIRNAME**

where **\$DIRNAME** is the absolute path of any existing directory.



Troubleshoot: For more Installation Troubleshooting, refer Troubleshooting page on our website.

Uninstalling Applications Manager

Windows:

1. Shut Down Applications Manager (Make sure that the ManageEngine ApplicationsManager service is stopped if installed as a Windows service)

2. Open a command prompt, go to Applications Manager Home directory (by default it is C:\Program Files\ManageEngine\AppManager) and execute the below commands,

```
shutdownApplicationsManager.bat
```

```
shutdownApplicationsManager.bat -force
```

3. Exit out of the command prompt and close all files, folders opened in the Applications Manager Home directory

4. Click Start > Programs > ManageEngine Applications Manager > Uninstall Applications Manager

5. Also from Control Panel > Add/Remove Programs.

Linux:

1. From the command line, go to Applications Manager Home directory (by default it is /opt/ManageEngine/AppManager) and execute the below commands

```
sh shutdownApplicationsManager.sh
```

```
sh shutdownApplicationsManager.sh -force
```

2. Exit out of the command prompt and close all files, folders opened in the Applications Manager Home directory

3. Execute the command *./uninstaller.bin* from the AppManager/_uninst directory.

Manually uninstalling Applications Manager

Refer the steps in the below link,

<http://apm.manageengine.com/manually-uninstall-Applications-Manager.html>

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.

Applying 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 **Licensing** 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: For **Enterprise Edition**, it is sufficient that you apply the license in Admin Server alone, the managed servers will be taken care automatically.

Note: The **Licensing** 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 the Admin tab.

Applying 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 appmanager-support@manageengine.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 9> 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 10> 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 **installservice.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. See this blog to get tips on starting Applications Manager when Linux boots.



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 10> Applications Manager Shutdown** (or)
- In Applications Manager's **Admin tab**, under **Tools**, click on **Shut Down Applications Manager** icon (or)
- Invoke **shutdownApplicationsManager.bat** file located in the *<Applications Manager Home>* directory (or)
- Right-click on the Applications Manager tray icon and click **Stop Applications Manager** (or)
- Click **Start > Run> services.msc> opens up Services console > stop ManageEngine Applications Manager**
[If Applications Manager is running as service]

In Linux

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

You can also use the **Shut Down Applications Manager** tool under Admin tab in Applications Manager.

Getting Started

When Applications Manager is started in Windows, 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 Applications Manager
- Prerequisites for Applications Manager
- Working with Applications Manager

You can also refer our Best Practices Guide for more help on getting started with Applications Manager.

Understanding Applications Manager

Applications Manager is a web-based monitoring tool that manages the performance of applications, servers, databases, systems, services, websites, and JMX/SNMP-based custom applications in a complex IT infrastructure.

You can find seven module tabs at the top which are explained as follows:

Intro	Introduction Page of Applications Manager. It gives an overview of the working of Applications Manager.
Home	<p>Has four views: <i>Summary</i>, <i>Business View</i>, <i>Availability</i> and <i>Performance</i></p> <p>Summary: Has a dashboard that shows the health and availability of all the Monitor Groups in a snapshot . Lists all the Monitor Groups created and their details and graphical representation of the Monitor Group with most critical alarms. Recent 5 alarms can be also be viewed.</p> <p>Business View: The business view provides you a graphical snapshot of the entire business infrastructure which is being monitored. This view displays the various Monitors associated to Monitor Groups along with its health and availability.</p> <p>Availability: Gives the Availability history of the Monitors/ Monitor Groups in a snapshot. You can get the data for either the last 24 hours or the last 30 days.</p> <p>Performance: Gives the Health history and events of Monitor/Monitor Groups in a dashboard. You can get the data for either the last 24 hours or the last 30 days (excluding today).</p> <p>Custom Dashboards: Apart from the already available dashboards, you can create your own custom dashboards by using different widgets.</p>
Monitors	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 Monitors. On clicking the Monitor Types, you can view the <i>Availability Dashboard</i> , <i>Performance Dashboard</i> and the <i>List View</i> that shows the performance attributes of the Monitor in detail.
Alarms	Lists the alarms generated by the Monitor and their attributes, based on predefined thresholds. The view is customizable such that you can view alarms for all or for particular application or Monitor Type, list 10/25/50/75/100/125 entries in a single view, etc.

Reports	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.
Support	Provides information on getting assistance from the Applications Manager Technical center. It also provides monitoring information on Applications Manager which monitors itself.
Admin	Lists the admin operations such as creating new application, new Monitor, etc. to be performed for monitoring.

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 Web Client section. The various tables in the web client can be dragged and arranged as per your requirement

Note: Have a look at Getting Started - How to Demos from Website.

Under Monitor tab, you can see all the monitors listed down. There are six different views

Category View	Lists the monitors according to the various categories like Applications Servers, Database Servers etc.,
Bulk Config View	Lists all the details of the monitors that are monitored. From this view you can carry out bulk admin operations like updating user name and passwords across monitors. Refer Bulk Configuration for further details.
Business View	<p>In this view, the Monitors will be arranged in an default order. You can re-arrange the Monitors and click on the floppy disk icon to save the view. You can also zoom in and out of the view, and save the zoom level which is optimal for your viewing.</p> <p>Business View has the following properties. You can edit the view by clicking on Settings icon and selecting the Edit View from the menu.</p> <ol style="list-style-type: none"> 1. Update Monitor - This setting allows you to refresh the status of the Monitors and Monitor Groups automatically by fixing some limited time (in minutes). 2. Reload Interval - This setting is similar to Update Monitor except that it will reload the entire view after the given time. The recommended interval would be 15 minutes. 3. Associated Monitor Groups - This setting allows you to add various Monitor Groups to your view. This is only available for the "Customizable Business View".

	<ol style="list-style-type: none"> Under View Properties, by selecting Show only Monitor Groups and Sub Groups allows you to include the Monitor Groups and Sub Groups in the selected view. By selecting Show only Critical Monitors you can show only critical Sub Groups and Monitors inside the selected view. By selecting Show only Monitor Groups Status you can show the status of top level Monitor Groups (that are selected via Associated Monitor Groups) in the selected view. <p>You can create multiple views for a Monitor Group. Click on the Settings icon in the business view and select Create New View. By providing various details like Update Monitor time interval, Reload interval, opting to select Monitor and Monitor Groups and Sub Groups you can create a custom view.</p> <p>In addition, you can also edit its appearance of the view. Go to the Display Properties tab and provide the following details:</p> <ol style="list-style-type: none"> Background color Line Color Label Color Line Thickness Line Transparency <p>Publishing the View: Applications Manager allows you to embed these Business View in intranet/internet portals by selecting the menu option '<i>Publish The View</i>' from Settings and copy the <i>iframe</i> details and pasting it in the webpages.</p>
World Map View	Applications Manager, integrated with online map services, provides network traffic information at a geographical dimension. By using online map API features, Applications manager provides different levels of abstraction in the network data visualization. Refer to World Map View for further details.
Icon View	Lists all the monitors using icons, shows the host and the monitors associated with it symbolically
Table View	Lists the monitors within the host in a tabular format.
Plasma View	<p>The plasma view enables you to have a snapshot of what is happening with the monitors, at one glance. The view can be put up on a plasma screen, and you can have a look even when you are not in front of the monitor.</p> <p>The 'Customize View' option available in the top right hand corner, gives you the option to customize the layout. By checking the option "Play sound alarm for critical events", you can get notified/ warned of the critical events by sound alarms.</p>

Monitor Group View	Lists all Monitor Groups and the Sub-Groups available. You can associate Monitors, Copy Paste Monitor, configure alarms through this Monitor Group View itself. (as like Bulk Config view). In addition, you can enable or disable actions via this view itself, i.e, even if you have already configured actions like sending EMail, through 'disable action' you can prevent EMail action.
---------------------------	--

Prerequisites for Applications Manager

Discussed below are the prerequisites for managing the various monitors:

- JBoss
- Tomcat
- WebLogic Integration Server
- WebLogic
- WebSphere
- SAP Server, SAP CCMS
- PHP
- Apache
- NTLM Authenticated URLs
- Oracle Application Server
- J2EE Web Transactions Monitor
- Java Runtime Monitor
- IBM WebSphere MQ
- Oracle EBS
- PostgreSQL

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.

To monitor JBoss 5.0.0 version and above *jbossagent.sar* should be deployed in JBoss server.

To deploy, follow the steps below

Copy jbossagent.sar from location **<Applications Manager home>/working/resources** and paste under **<JBOSS_HOME>/server/default/deploy**. If you are running JBoss in different domain like *all*, then deployment target folder would be **<JBOSS_HOME>/server/all/deploy**

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

WebLogic Integration Server

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

- For monitoring **WebLogic Integration Server 8.x**, you should set the **weblogic.disableMBeanAuthorization** and **weblogic.management.anonymousAdminLookup** system variable to **true** for enabling data collection. Follow the steps given below:
 1. Edit **startWLS.cmd\sh** present in the `<WLS_HOME>/server/bin` directory and add the following argument **-Dweblogic.disableMBeanAuthorization=true** and **-Dweblogic.management.anonymousAdminLookupEnabled=true** (click on the link to view the sample **startWLS.cmd\sh** file)
 2. Restart the WebLogic Integration Server for the changes to take effect.
 3. Copy **weblogic.jar** from folder `/weblogic81/server/lib` in Remote WebLogic server version 8 and place it under `<AppManager Home>\workingclasses\weblogic\version8` folder in the machine where Applications Manager is running.

WebLogic

To monitor WebLogic 6.1 ,

Follow the steps given below:

- 1) Provide only Admin user name.
- 2) Copy **Weblogic.jar** from folder `<Weblogic Home>/weblogic61/server/lib` in Remote WebLogic server version 6. Copy to `<AppManager Home>\workingclasses\weblogic\version6` folder in the machine where Applications Manager is running

To monitor WebLogic 7.x:

You should set the *weblogic.disableMBeanAuthorization* and *weblogic.management.anonymousAdminLookupEnabled* variables 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 arguments
-Dweblogic.disableMBeanAuthorization=true
-Dweblogic.management.anonymousAdminLookupEnabled=true Click here for Sample startWLS.cmd/sh
- 2) Restart the WebLogic Server for the changes to take effect
- 3) Copy *Weblogic.jar* from folder *<Weblogic Home>/weblogic70/server/lib* in Remote WebLogic server version 7. Copy to *<AppManager Home>\working\classes\weblogic\version7* folder in the machine where Applications Manager is running

To monitor WebLogic 8.x

You should set the *weblogic.disableMBeanAuthorization* and *weblogic.management.anonymousAdminLookupEnabled* variables 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 arguments
-Dweblogic.disableMBeanAuthorization=true
-Dweblogic.management.anonymousAdminLookupEnabled=true Click here for Sample startWLS.cmd/sh
- 2) Restart the WebLogic Server for the changes to take effect
- 3) Copy *Weblogic.jar* from folder *<Weblogic Home>/weblogic81/server/lib* in Remote WebLogic server version 8 Copy to *<AppManager Home>\working\classes\weblogic\version8* folder in the machine where Applications Manager is running.

To monitor WebLogic 9.x ,

Copy *Weblogic.jar* from folder *<Weblogic Home>/weblogic92/server/lib* in Remote WebLogic server version 9 . Copy to *<AppManager Home>\working\classes\weblogic\version9* folder in the machine where Applications Manager is running.

To monitor WebLogic 10.x ,

Copy *Weblogic.jar*, *wlclient.jar*, *wljmsclient.jar* from folder <Weblogic Home>/wlserver_10.0/server/lib in Remote WebLogic server version 10 .Copy to <AppManager Home>\working\classes\weblogic\version10 folder in machine where Applications Manager is running.

WebSphere Application Server**For base deployment:**

You have to modify the Performance Monitor Interface (PMI) Specification Level from "None" to "Standard". Then deploy the *perfServletApp.ear* file, which uses the PMI infrastructure to retrieve the performance information from WebSphere Application Server, in the WebSphere. Restart WebSphere Application Server.

For Network deployment:

You have to modify the PMI Sepcificiaion Level from "None"to "Standard" in all the WebSphere Servers in Network Deployment. Then deploy the *perfServletApp.ear* file, which uses the PMI infrastructure to retrieve the performance information from WebSphere Application Server, in any one of the WebSphere Servers in the Network Deployment. Restart WebSphere Application Server.

Note: Steps to check whether WebSphere monitor has been correctly set.

To modify PMI specification level:

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

To deploy 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 WebSphere installation directory).
- Restart WebSphere Server.

Steps to Check whether Websphere monitor has been correctly set

For Base Deployment

To ensure whether the **PMI & perfServletApp** are configured properly in WebSphere, invoke the below URL & check whether the data is returned in XML format.

http://WebSphereHost:Port/wasPerfTool/servlet/perfservlet?connector=SOAP&port=SOAP-PORT
where

WebSphere Host -> Host in which WebSphere Application Server is running

WebSphere Port -> HTTP Transport port of the WebSphere Application server [How to locate HTTP Port]

SOAP Port -> SOAP Port of WebSphere [How to locate SOAP Port]

For Network Deployment

To ensure whether the **PMI & perfServletApp** are configured properly in WebSphere, invoke the below URL & check whether the data is returned in XML format.

http://WebSphereHost:Port/wasPerfTool/servlet/perfservlet?connector=SOAP&port=NetworkDeployer SOAP-PORT&HOST=NetworkDeployerHost

WebSphere Host -> The host of the websphere application server in which the perf servlet application is installed

WebSphere Port -> HTTP Transport port of the Websphere server in which the perf servlet application is installed [How to locate HTTP Port]

NetworkDeployer SOAP PORT -> The SOAP port of the domain manager (DMGR) [How to locate SOAP Port]

Network Deployer Host -> The host in which the domain manager is running.

Note: Also check whether WebSphere *admin user* is added to the monitor group of the **perfservletApp**.

How to locate SOAP Port?

1. Login to Admin console
2. Expand the *server* link on left side tree. Click on *Application Servers*
3. In *Base mode*, various WebSpheres will be listed down. Click on the WebSphere's name- > Under *Additional Properties*, click on *End Points* link -> click on *SOAP connector address*. You can get the SOAP port from there.
4. In *Network Deployment mode*, Click DMGR - > Under *Additional Properties*, click on *End Points* link -> click on *SOAP connector address* - You can get the SOAP port from there.

How to find the HTTP Transport port?

1. Login to Admin console
2. Expand the *Server* link on left side tree, Click on *Application Servers*
3. Various WebSpheres will be listed down. Click on the WebSphere's name- > Under *Additional Properties*, click on *Web Container* link -> click on *HTTP Transports* link. You can get the HTTP port from there.

SAP Server, SAP CCMS

SAP Server Monitoring and SAP CCMS Monitoring requires SAP JavaConnector (JCo) to be present in Applications Manager's classpath.

For Windows:

1. Download latest **SAP JavaConnector** [*sapjco-ntintel-2.1.8*] from <http://service.sap.com/connectors>. Unzip the file.
2. In the machine, where AppManager is running, Copy *librfc32.dll* to *C:\WINDOWS\system32* directory. Copy *sapjcorfc.dll* and *sapjco.jar* to *AppManager10/working/lib* directory.
3. Verify *msvcr71.dll* and *msvcpr71.dll* exist in the Windows system directory. The DLL files must be added to the Windows system directory if they do not already exist.
4. Restart Applications Manager by running *startApplicationsManager.bat* file.

Note: Not able to add SAP Monitor in **Windows Vista**? The reason is that *msvcr71.dll* and *msvcpr71.dll* files are not present in the Windows Vista machine. Copy those dlls from any other windows XP machine to vista machine (*c:\windows\system32*).

Still not able to add? Create Support Information File and send it to appmanager-support@manageengine.com.

For Linux:

1. Download latest **SAP JavaConnector** [*sapjco-linuxintel-2.1.8.tar*] from <http://service.sap.com/connectors>. Unzip *libsapjcorfc.so*, *sapjco.jar* and *librfccm.so* under *AppManager10/working/lib* directory. Verify if *libstdc++-libc6.2-2.so.3* is available under */usr/lib/* directory.
2. Restart Applications Manager by running *startApplicationsManager.sh* file
3. The user name provided while adding SAP monitor **should have** sufficient privileges to access CCMS metrics. To check this, the user can execute **RZ20 transaction** in the SAP GUI and see if the CCMS monitor sets can be displayed.

PHP

Place the *phpstats.php* file in the webserver's document root. The *phpstats.php* can be found in *<Applications Manager Home>/working/resources* directory.

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.

NTLM Authenticated URLs

To monitor **NTLM** authenticated URLs,

- Download cryptix-jce-20050328-snap.zip file from <http://www.cryptix.org/cryptix-jce-20050328-snap.zip>
- Extract the contents of the cryptix-jce-20050328-snap.zip file to any location and copy the *cryptix-jce-provider.jar* file under *..\bin* folder to *Applications Manager Home\lib\ext*.
- Restart Applications Manager.

Oracle Application 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://docs.oracle.com/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*.

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

- 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/dms0/AggreSpy> from the Applications Manager system. To understand how to enable access to the above URL, visit the link given below and navigate to page 15 - PROTECT ADMINISTRATIVE WEB PAGES.

http://erpseminars.com/files/Note189367_1.pdf

J2EE Web Transactions

J2EE Web Transaction Monitor requires an **agent** to be plugged in the application server (like JBoss) to be monitored. Know more about the J2EE Web Transactions Agent.

Java Runtime Monitor

To monitor a JDK1.5 JVM and above, the following java runtime options needs to be added to your application

`-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=1099 -`

`Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false`

<p>Note: Port number '1099' can be replaced with the actual port number of the JMX agent..</p>

IBM WebSphere MQ Monitor

For monitoring IBM Websphere MQ version 5 and version 6, three jar files are required-

com.ibm.mq.jar, **com.ibm.mq.pcf-6.x.jar** and **connector.jar**. For monitoring Version 7, three more jar files should be added.

Follow the below steps to get these jar files and copy them to the product.

1) Download the **supportpac MS0B** : WebSphere MQ Java classes for PCF from the following link <http://www-1.ibm.com/support/docview.wss?uid=swg24000668> . From this support pac, you can get the **com.ibm.mq.pcf-6.x.jar** file .

2) **com.ibm.mq.jar** and **connector.jar** can be located at <Websphere MQ Home Directory>\Java\lib directory.

3) Copy the three jar files to <ProductHome>\working\jre\lib\ext directory and restart Applications Manager and try adding the monitor again.

4) For monitoring Version 7, additionally you need to copy the following jar files from <websphere mq series installation>\java\lib directory to <AppManager Installation>\working\jre\lib\ext directory

i)**com.ibm.mq.headers.jar**

ii)**com.ibm.mq.commonservices.jar**

iii)**com.ibm.mq.jmqi.jar**

Oracle EBS

Applications Manager uses the **Dynamic Monitoring Service (DMS)** provided by Oracle E-Business Suite 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://docs.oracle.com/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 by modifying the *\$ORACLE_HOME/Apache/Apache/conf/dms.conf* file in UNIX or *%ORACLE_HOME%\Apache\Apache\conf\dms.conf* in Windows systems.

The example below shows a sample default configuration from *dms.conf* file. This configuration limits *AggreSpy* to access metrics on the localhost (127.0.0.1). The port shown (7200) may differ in 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*.

Caution: Modifying *dms.conf* has security implications. Modify this file only 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:

1. Modify *dms.conf* file 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*).
2. 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

- 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/dms0/AggreSpy> from the Applications Manager system. To understand how to enable access to the above URL, visit the link given below and navigate to page 15 - PROTECT ADMINISTRATIVE WEB PAGES.

http://erpseminars.com/files/Note189367_1.pdf

PostgreSQL

Applications Manager uses PostgreSQL's subsystem statistics collector to monitor PostgreSQL server activity. By default, the statistics collector is accessible.

If you have problems in adding a new PostgreSQL server, follow the steps given below:

- Open `postgresql.conf` under `<postgres home>/data`
- Check value of configuration parameter **listen address** it has to be `""`, if not change it to `""`.
Click here for more details on configuring `postgresql.conf`
- Open `pg_hba.conf` under `/data`
- Add a new line `host all all 0.0.0.0/0 md5` to allow all machines with proper password authentication to access PostgreSQL DB server. Click here for more details on configuring `pg_hba.conf`

For any further support please contact appmanager-support@manageengine.com. You can visit Troubleshooting details.

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. Create new Monitor Type: Create new monitor type for monitoring custom applications.
4. Associate Monitor with Monitor Group: Add the discovered monitors to the Monitor Group.
5. Create threshold profile: Create thresholds to identify the status of a specific attribute.
6. Create actions: Specify what action needs to be taken in the event of an alarm.
7. Associate threshold and action with the attributes: Associate the thresholds and action to generate alarms and perform action based on the threshold definition.
8. 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.

Note: Have a look at Working with Applications Manager - How to Demos from the website.

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

See Also

Best Practices Guide

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:

- Creating Monitor Groups
- Creating Web Application Groups
- Creating New Monitor
- Associating Monitors to Monitor Groups
- Deleting Monitor from Monitor Groups
- Editing and Deleting a Monitor Group

Creating Monitor Groups

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.

Applications Manager provides two types of monitor groups - Monitor Group and Web Application Group. The steps to create a Monitor group are explained below. To create a web application group, refer this link.

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:

Operator if associated as an owner will have Read Only Access to that particular Monitor Group alone.

Admin user is a super user and will be able to see all Monitor Groups.

Manager if associated will be able to view this Monitor Group in Manager Console. Using this option, Restricted Monitor Groups alone can be shown in Manager Console. [By default, if the Manager is not explicitly associated to a Monitor Group, the Manager will be able to access all the Monitor Groups in the Manager Console]

5. Select the **location** for associating the monitor group to World Map Business View. Else by clicking on 'Add Location', world map opens up. Here you can add and select custom locations.
6. Click **Finish** to create the Monitor Group and to add Monitors later.

How To Demos: Have a look at our demo on creating Monitor Group in our website.

Creating a Sub-Group within a Monitor Group

By using this option, you can create a Monitor Sub-Group within a Monitor Group (a Monitor Group within a Monitor Group). Sub-Groups help better organization of your resources. With Sub-Groups, you can capture advanced dependencies in your infrastructure. You can group clustered databases or servers and create complex groups. For eg., A huge banking application Monitor Group may contain 100 monitors (application servers, systems, databases, URLs, etc.). All the database monitors can be grouped under a Sub-Group for effective monitoring.

To create a sub group,

- Inside the Monitor Group Details page, click on New Sub-Group link on the left.
- Give the Sub-Group name and the description.
- Click on 'Create Sub-Group'.
- Then you can associate the desired monitors to the Sub-Group.

Note: You can create up to six levels of sub-groups in a Monitor Group, by default.

Creating New Web Application Group

A web application group provides a template for grouping web infrastructure into logical components. So, instead of manually grouping your web infrastructure, you can use the web application group to categorize your infrastructure into servers, databases, web servers, etc.

Once you create a web application group, you can view the health of the sub groups and know how each individual sub group is performing. If there is a problem in the web application group, you can drill down and identify which component is having a problem. The details page shows the health of all the tiers as components giving you a better perspective of the Application's Performance and Availability. You can also configure dependencies and powerful alarm rules for intelligent alert correlation.

To create a new web application group, follow the steps given below:

1. Click **New Monitor Group** and select **Web Application Group** from the drop-down menu.
2. Provide a **Name** for the Monitor Group. This is mandatory and only alphanumeric characters, dashes (-), underscores (_), periods (.), and spaces () are allowed.
3. Provide a **Description**, if required.
4. Select the **Owner** from the list of users displayed. Refer User Administration topic for more information on the different roles of users.

Note:

Operator if associated as an owner will have Read Only Access to that particular Monitor Group alone.

Admin user is a super user and will be able to see all Monitor Groups.

Manager if associated will be able to view this Monitor Group in Manager Console. Using this option, Restricted Monitor Groups alone can be shown in Manager Console. [By default, if the Manager is not explicitly associated to a Monitor Group, the Manager will be able to access all the Monitor Groups in the Manager Console]

5. Select **Web Application Group** as the group type.
6. Select the **Application Components** from the options displayed. The components available are End User Transaction (URL) group, Network devices group, Edge Devices group, Web Server Group, Application Server Group, Database Group and Server Group. The components that you select will be automatically added as sub groups within the web application group.
7. Select the **Location** for associating the monitor group to World Map Business View under *Advanced* section. Otherwise, click the 'Add Location' link and select custom locations from the google map that opens up.
8. Click **Create Monitor Group** button to create the Web Application Group. You can add monitors any time using the *Associate Monitors* option.

Note: You can convert a web application group to a monitor group or vice versa by changing the **Group Type**. Click **Monitor Group Options** link from the web application group page and select the **Edit** option. This will take you to the *Modify Monitor Group* section. You can modify the Group Type values from this screen.

Creating a Sub-Group within a Web Application Group

If you have selected 'Application Components' while creating the web application group, the sub groups will be automatically created based on the options you have selected. You can also add sub groups later on by following the steps given below.

- Click the **Monitor Group Actions->New Sub-Group** option inside the Web Application Group Details page.
- Provide the *Sub-Group Name, Description* and select the *Owner* from the list of users.
- Select the *Group Type* from the dropdown box.
- Select the *Location* for associating the sub group to from the drop-down box. You can also use the 'Add Location' option to specify custom locations from google map.
- Click the *Create Sub-Group* button to create the sub group.
- You can then associate the desired monitors to the Sub-Group.

Note: You can create up to six levels of sub groups for a web application group, by default.

VMware Virtual Infrastructure Groups

Applications Manager can discover your entire VMware virtual infrastructure through the vCenter server and provide dependency mapping of its components. The 'VMware Virtual Infrastructure Group' allows you to quickly discover all your virtual resources and model them the same way they are configured in the vCenter server. The VMware infrastructure will be automatically categorized into components such as Datacenter, Cluster, ESX/ESXi hosts, VMs, etc. Once you discover the virtual infrastructure, you can easily track the availability, health and performance metrics of its various components.

The VMware virtual infrastructure group is different from monitor groups due to the fact that you have to manually map all the resources to a monitor group. In the VMware virtual infrastructure group, the virtual resources in your network are automatically discovered through the vCenter server and the components mapped accordingly. When combined with the out-of-the-box support for 50+ applications, servers, databases, and transactions spanning physical, virtual and cloud infrastructures along with auto-provisioning of virtual systems, the VMware virtual infrastructure group becomes even more powerful.

Creating a New VMware Virtual Infrastructure Group

Follow the steps given below to create a VMware Virtual Infrastructure group:

1. Click **New Monitor Group** and select **VMware Virtual Infrastructure** from the drop-down menu. The 'Discover Virtual Infrastructure through vCenter' screen will be displayed.
2. Provide a **Display Name** for the monitor group.
3. Specify **vCenter Hostname/IP Address**.
4. Specify the **Port** at which vCenter is running.
5. Enter the authentication credentials of the vCenter server such as **User Name** and **Password**.
6. Specify the **Polling Interval** in minutes.
7. Click **Fetch ESX Hosts** button to start the virtual infrastructure discovery.

For more information on the performance metrics provided by the VMware virtual infrastructure group, refer this topic.

Associating Monitors to Monitor Groups

To associate a 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.
Note: The status of Monitor Group would remain Unknown, until you associate atleast one monitor to it.
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**.

Note: Network Devices can now be monitored out-of-the-box using the ManageEngine OpManager Network Monitoring Connector.

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**.

Editing and Deleting a Monitor Group

To edit a Monitor Group,

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

By editing the monitor group, you can change the Name, Description, Owners and the Country (location) associated.

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: In simple layout, the left side links will not be present. In this case, move to *Monitors* tab, from Select View drop down box, select *Monitor Group* view. Select the Monitor Groups you want to delete, then select the *Delete* action from the dropdown.

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

Configuring New Monitor

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 starts **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 any of the options given below:

- All Monitors in a host.
- A specific Monitor in a host.
- All Monitors in a network

Note: If there is a problem while creating new monitors, click on **Diagnose** link to troubleshoot the problem

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**.
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

Note: Adding any service will also automatically add that server and other applications in the default port in that server.

How To Demos: Have a look at our demo on creating Monitors in our website.

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

- Application Servers

- Database Servers
- MiddleWare/Portal
- Services
- Mail Servers
- Web Server/Services
- Servers
- URL Monitoring
- Oracle E-Business Suite
- SAP Server
- SAP CCMS
- Virtualization Monitor
- Amazon Monitor
- Custom Monitor
- File/Directory Monitor
- Windows Performance Counters
- Script Monitor
- Database Query Monitor
- J2EE Web Transactions Monitor
- JMX/SNMP Dashboard
- Network Monitoring Connector

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
- GlassFish Server
- JBoss Server
- Oracle Application Server
- SilverStream
- Tomcat Server
- VMware vFabric tc Server
- WebLogic Server
- WebSphere Server

Microsoft .NET

To create Microsoft .NET Monitor

1. Click on **New Monitor** link.
2. 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 / Domain 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.

GlassFish Server

To create GlassFish Application Server Monitor

1. Click on **New Monitor** link.
2. Select **GlassFish**.
3. Give the **Display name**.
4. Enter the **Hostname** of the host where GlassFish runs.
5. Enter the **Port**
6. Enter the **User Name** and **Password** of GlassFish Server.
7. Enter the **JNDI** path.
8. Set the **Polling Interval**.
9. Choose the **Monitor Group** from the combo box with which you want to associate GlassFish Monitor (optional).
10. Click **Add Monitor(s)**. This discovers GlassFish Servers from the network and starts monitoring them.

JBoss Server

Supported versions of JBoss Server: 3.2.x, 4.x, 4.0.x, 5, 5.1

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 on **New Monitor** link.
2. 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 on **New Monitor** link.
2. 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.

SilverStream

To create a SilverStream Server Monitor

1. Click on **New Monitor** link.
2. Select **SilverStream**.
3. Give the **Display name**.
4. Enter the **Hostname** of the host where SilverStream Server runs.
5. Enter the **Port number**.
6. Set the **Polling interval**.

7. Choose the **Monitor Group** from the combo box with which, you want to associate SilverStream Server Monitor (optional).
8. Click **Add Monitor(s)**. This discovers SilverStream Server from the network and starts monitoring them.

Tomcat Server

The supported versions of Tomcat Servers are 3.x, 4.x, 5.x, 6.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).

```
<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).

```
<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

- o *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 on **New Monitor** link.
2. 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 and above, 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 and above) 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 <JBoss_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> "
```

2. Restart the JBoss server.
3. Configure a tomcat monitor by clicking New Monitor --> Select Tomcat Server in the combo box.
- 4.
5. 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.

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: *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.

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 appmanager-support@manageengine.com if you would like to have it added.

VMware vFabric tc Server

To create VMware vFabric tc Server Monitor

1. Click on **New Monitor** link.
2. Select **VMware vFabric tc Server**.
3. Provide the **Display name** of the monitor.

4. Enter the **Host Name** in which the vFabric tc Server is running.
5. Enter the **Port** number in which the JMX Agent is running (6969 by default). The port in which JMX agent is running; is defined in the 'catalina.properties' file.
6. Enter the **User Name** and **Password** of the vFabric tc Server.
7. Specify the **JNDIPath**. For example, JNDIPath for default installations of vFabric tc Server is /jmxrmi.
8. Specify the **Polling Interval** in minutes.
9. Choose the **Monitor Group** from the combo box with which you want to associate vFabric tc Server Monitor (optional).
10. Click **Add Monitor(s)**. This discovers the vFabric tc Server from the network and starts monitoring it.

Note: To enable JMX in the tc Server, you have to define a JMX port in the file 'catalina.properties' and then give an entry in a *server.xml*

[Click the link to view an example server.xml file and also a snippet of catalina.properties which shows how to set values for the variables used in the server.xml file].

WebLogic Server

The supported versions of WebLogic Servers are 6.1, 7.x, 8.x, 9.x, 10.x.

Know the Prerequisites that are required to monitor WebLogic.

To create a WebLogic Server Monitor

1. Click on **New Monitor** link.
2. 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 **user name and password**.

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

- **To monitor WebLogic 6.1 ,**

Follow the steps given below:

- 1) Provide only Admin user name.
- 2) Copy **Weblogic.jar** from folder <Weblogic Home>/weblogic61/server/lib in

Remote WebLogic server version 6. Copy to <AppManager Home>\working\classes\weblogic\version6 folder in the machine where Applications Manager is running

To monitor WebLogic 7.x ,

You should set the *weblogic.disableMBeanAuthorization* and *weblogic.management.anonymousAdminLookupEnabled* variables 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 arguments
-Dweblogic.disableMBeanAuthorization=true
-Dweblogic.management.anonymousAdminLookupEnabled=true Click here for Sample startWLS.cmd/sh
- 2) Restart the WebLogic Server for the changes to take effect
- 3) Copy Weblogic.jar from folder <Weblogic Home>/weblogic70/server/lib in Remote WebLogic server version 7. Copy to <AppManager Home>\working\classes\weblogic\version7 folder in the machine where Applications Manager is running

To monitor WebLogic 8.x

You should set the *weblogic.disableMBeanAuthorization* and *weblogic.management.anonymousAdminLookupEnabled* variables 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 arguments
-Dweblogic.disableMBeanAuthorization=true
-Dweblogic.management.anonymousAdminLookupEnabled=true Click here for Sample startWLS.cmd/sh
- 2) Restart the WebLogic Server for the changes to take effect
- 3) Copy Weblogic.jar from folder <Weblogic Home>/weblogic81/server/lib in Remote WebLogic server version 8 Copy to <AppManager Home>\working\classes\weblogic\version8 folder in the machine where Applications Manager is running.

To monitor WebLogic 9.x ,

Copy Weblogic.jar from folder <Weblogic Home>/weblogic92/server/lib in Remote WebLogic server version 9 . Copy to <AppManager Home>\working\classes\weblogic\version9 folder in the machine where Applications Manager is running.

To monitor WebLogic 10.x ,

Copy *Weblogic.jar*, *wlclient.jar*, *wljmsclient.jar* from folder *<Weblogic Home>/wlserver_10.0/server/lib* in Remote WebLogic server version 10 .Copy to *<AppManager Home>\working\classes\weblogic\version10* folder in machine where Applications Manager is running.

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.

Prerequisites for Websphere Monitoring: For Applications Manager to collect data from WebSphere Application Server, configurations are required at the Performance Monitoring Infrastructure (PMI) specification level. Refer **Prerequisites Section** for configuration details.

To create a WebSphere Server Monitor

1. Click on **New Monitor** link.
2. 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 in which websphere application server is running.
For Network Deployment, enter the Host name/IP Address of the websphere application server in which the perf servlet is installed. 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).
10. If you want to monitor WebSphere through SSL mode, select the **SSL is enabled** checkbox.
11. Enter the User Name and Password, if Global Security is enabled.

12. In Network Deployment Mode, Enter the **Network Deployer's Host and SOAP Port (Default : 8879)**.
13. Choose the **Monitor Group** from the combo box with which you want to associate WebSphere Server Monitor (optional).
14. Click **Add Monitor(s)**. This discovers WebSphere server from the network and starts monitoring them.

Note: Applications Manager has been tested for WebSphere versions of English, German, Japanese and Chinese languages.



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

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
- Oracle
- MS SQL
- IBM DB2
- Sybase
- PostgreSQL
- Memcached

MySQL Database Server

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.

Minimum User Privileges : The user should have privileges to execute SELECT, SHOW DATABASES, REPLICATION commands in the MySQL server. Also, Applications Manager machine should be allowed to access the MySQL database server.

For enabling the privileges, execute the below commands in the remote MySQL Server

```
INSERT INTO user (Host,User) VALUES('<host>','<user>');  
GRANT SELECT,SHOW DATABASES,REPLICATION CLIENT ON *.* TO '<user>'@'<host>';  
FLUSH PRIVILEGES;
```

(Host -> Applications Manager machine) /

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

1. Click on **New Monitor** link.
2. 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.



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:

Note: For you to create a new Oracle database monitor, you should have admin privileges. Minimum User Privileges -> user with CONNECT and SELECT_CATALOG_ROLE roles

1. Click on **New Monitor** link.
2. 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 **System Identifier / Host Connection String**.

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.

MS SQL Database Server

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

1. Click on **New Monitor** link.
2. 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. Alternatively, you can provide the **Windows Authentication** details (give the User Name like domainname\username) also.
8. Choose the **Monitor Group** from the combo box with which you want to associate MS SQL database server Monitor (optional).
9. Click **Add Monitor(s)**. This discovers MS SQL database server from the network and starts monitoring them.

Note:

Minimum User Privileges: User should be permitted to access MASTER database & MSDB database.

Roles: public + db_datareader should be selected for both MASTER and MSDB databases.

For MS SQL 2005 and 2008 user roles:

Database Accessed: Master

Permit in Database Role: db_datareader & Requires **VIEW SERVER STATE** permission on the server.

To grant **VIEW SERVER STATE**, you can use any of the following methods :

1) Execute the following query

GRANT VIEW SERVER STATE TO username;

2) In SQL management studio for user choose Properties -> Securables -> Click **Add** (under securables) -> choose "**All objects of the Types...**" -> choose **Servers** -> choose **Grant** for "**View server state**" permission.

IBM DB2 Database Server

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

Note: IBM DB2 ver.8 and ver.9 monitoring is supported. And also, you should be able to access the SYSPROC procedures.

1. Click on **New Monitor** link.
2. 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 DB2 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 DB2 database server Monitor (optional).
10. Click **Add Monitor(s)**. This discovers DB2 database server from the network and starts monitoring them.

Sybase Database Server

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

Note: Sybase ASE ver.12.5.3 and above monitoring is only supported.

1. Click on **New Monitor** link.
2. Select **Sybase**.
3. Enter the **IP Address** or **Host Name** of the host.
4. Enter the SubNetMask of the network.
5. Enter the **port number** in which sybase 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 Sybase database. The user name specified for collecting the data from Sybase 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 Sybase database server Monitor (optional).
10. Click **Add Monitor(s)**. This discovers Sybase database server from the network and starts monitoring them.

PostgreSQL Database Server

To create a PostgreSQL database server monitor, follow the steps given below:

1. Click on **New Monitor** link.
2. Select **PostgreSQL**.
3. Enter the **Display Name** of the database server.
4. Enter the **IP Address** or **Host Name** of the host.
5. Enter the **port number** in which PostgreSQL is running.
6. Provide the **user name** and **password** of user who has permission to access the PostgreSQL database.
7. Specify the **DBName**.
8. Enter the polling interval time in minutes.
9. Choose the **Monitor Group** with which you want to associate the PostgreSQL database server to, from the combo box (optional).
10. Click **Add Monitor(s)**. This discovers PostgreSQL database server from the network and starts monitoring them.

Memcached Server

To create a Memcached database server monitor, follow the steps given below:

1. Click on **New Monitor** link.
2. Select **Memcached** under Cloud Computing/Virtualization category.
3. Specify the **Display Name** of the memcached server
4. Enter the **HostName** or **IP Address** of the host where Memcached server runs.
5. Enter the **Port** where the server is running.
6. If you want to enable Transaction test, select 'Yes' radio button, otherwise select 'No' button.
7. Set the **Polling Interval**.
8. Choose the **Monitor Group** with which you want to associate the Memcached server to, from the combo box (optional).
9. Click **Add Monitor(s)**. This discovers the Memcached server from the network and starts monitoring it.

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](#)

Middleware / Portal

Applications Manager monitors middleware software servers and applications to detect performance problems before they could affect the system..

The following are the different Middleware / Portals supported by Applications Manager:

- Microsoft MQ (MSMQ)
- WebLogic Integration
- IBM WebSphere MQ [Add On!](#)
- Microsoft Office SharePoint Server [Add On!](#)
- VMware vFabric RabbitMQ

Microsoft MQ (MSMQ)

Follow the steps given below to create a new Microsoft MQ monitor:

1. Click on **New Monitor** link.
2. Select **Microsoft MQ (MSMQ)** under Middleware/Portal category.
3. Enter the **Display Name** of the host.
4. Provide the monitor-specific authentication information, such as **User Name and Password**.
5. Enter the polling interval time in minutes.
6. Choose the **Monitor Group** with which you want to associate the Microsoft MQ server to, from the combo box (optional).
7. Click **Add Monitor(s)**. This discovers Microsoft MQ server from the network and starts monitoring it.

WebLogic Integration Server

The supported version of WebLogic Integration Server is 8.x.

Important: Know the **Prerequisites** that are required to monitor WebLogic Integration Server.

To create a WebLogic Integration Server Monitor

1. Click on **New Monitor** link.
2. Select **WebLogic Integration**.
3. Enter the **IP Address/ hostname** of the host.
4. Enter the SubNetMask of the network.

5. Enter the **port number** in which WebLogic Integration Server is running.
6. Enter the polling interval time in minutes.
7. Provide the monitor-specific authentication information, such as **user name and password**.

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

- For monitoring **WebLogic Integration Server 8.x**, you should set the **weblogic.disableMBeanAuthorization** and **weblogic.management.anonymousAdminLookup** system variable to **true** for enabling data collection. Follow the steps given below:
 1. Edit **startWLS.cmd\sh** present in the `<WLS_HOME>/server/bin` directory and add the following argument **-Dweblogic.disableMBeanAuthorization=true** and **-Dweblogic.management.anonymousAdminLookupEnabled=true** (click on the link to view the sample **startWLS.cmd\sh** file)
 2. Restart the WebLogic Integration Server for the changes to take effect.
 3. Copy **weblogic.jar** from folder `/weblogic81/server/lib` in Remote WebLogic server version 8 and place it under `<AppManager Home>\working\classes\weblogic\version8` folder in the machine where Applications Manager is running.

8. Choose the **Monitor Group** from the combo box with which you want to associate WebLogic Integration Server Monitor (optional).
9. Click **Add Monitor(s)**. This discovers WebLogic Integration server from the network and starts monitoring them.

IBM WebSphere MQ

To create a IBM WebSphere MQ Monitor

Important: Know the **Prerequisites** that are required to monitor IBM WebSphere MQ.

1. Click on **New Monitor** link.
2. Select **IBM WebSphere MQ**.
3. Give the **Display Name**.
4. Enter the **Hostname** of the host where IBM WebSphere MQ runs.
5. Enter the **Listener Port**
6. Enter the **ServerConnection Channel**
7. Set the **Polling Interval**.
8. Choose the **Monitor Group** from the combo box with which you want to associate IBM WebSphere MQ Monitor (optional).

9. Click **Add Monitor(s)**. This discovers IBM WebSphere MQ from the network and starts monitoring them.

Microsoft Office SharePoint Server

To create a Office Share Point Server Monitor

1. Click on **New Monitor** link.
2. Select **MS Office SharePoint**.
3. Give the **Display Name**.
4. Enter the **Hostname** of the host where Office Share Point Server runs.
5. Enter the **Username** and **Password** for the server.
6. Set the **Poll** interval.
7. Choose the **Monitor Group** from the combo box with which you want to associate MS Office SharePoint server (optional).
8. Click **Add Monitor(s)**. This discovers MS Office SharePoint server from the network and starts monitoring them.

VMware vFabric RabbitMQ Server

To create a RabbitMQ Server Monitor:

1. Click on **New Monitor** link.
2. Select **RabbitMQ** under the **Middleware/Portal** list.
3. Enter the **Display Name** and the name of the **host** where the RabbitMQ Server is running.
4. Enter the **Port** ID where the management plugin is configured. For default installations of RabbitMQ management plugin, the port number is 55672.
5. Enter the correct **User Name** and **Password** of RabbitMQ server.
6. Set the **polling interval**.
7. Select the **Monitor Group** from the combo box with which you want to associate RabbitMQ server (optional).
8. Click **Add Monitor(s)**. This identifies RabbitMQ server from the network and starts monitoring.

See Also

Monitor Information - Middleware / Portal | Create Other New Monitors

Services

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

- JMX Applications
- Ping Monitor
- Service Monitoring
- SNMP
- Telnet
- Active Directory
- DNS Monitor
- FTP/SFTP Monitor
- LDAP Monitor

JMX Applications

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

1. Click on **New Monitor** link. Choose **JMX Applications**.
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. If Authentication is enabled, enter the Username and password.
8. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
9. Click **Add Monitor(s)**. This discovers the **Monitor** from the network and starts monitoring them.

Ping Monitor

To create a Ping monitor, follow the steps given below:

1. Click on **New Monitor** link. Choose **Ping Monitor** under 'Services' category.
2. Provide **Host Name / IP Address**.

3. Enter the **Timeout** value for the monitor in seconds.
4. Specify the **Polling Interval** for the monitor in minutes.
5. Select the **Monitor Group** with which you want to associate the monitor to, from the combo box (optional).
6. Associate the monitor instance to the agent.
 1. Enable **Run on Server** option to run the ping monitor in the local instance of Applications Manager.
 2. Enable **Run on Agent** option to run the ping monitor from multiple locations. Select the necessary agents from where you want this monitor to be executed. This option will be available only if you enable the EUM add-on.
7. Click **Add Monitor(s)**. This adds the ping monitor and the monitoring will be started as per the polling interval configured.

Service Monitoring

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

1. Click on **New Monitor** link. 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 / HTTP1.0 . 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.

SNMP (v1 or v2c)

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

1. Click on **New Monitor** link. 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 on **New Monitor** link. 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.

Active Directory

To create an Active Directory Monitor, follow the given steps:

1. Click on **New Monitor** link. Choose **Active Directory** under **Services**.
2. Enter the **DisplayName** of the host in which the Monitor is running.
3. Enter the **HostName** on which the monitor is running.
4. If Authentication is enabled, enter the **Username** and **Password**.
5. Provide the **Polling interval** for monitoring the Active Directory monitor.
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 **Monitor** from the network and starts monitoring them.

Note: Kindly ensure that for User accounts, relevant privileges must be provided before creating Active Directory monitor. 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.

DNS Monitor

To create an DNS Monitor, follow the given steps:

1. Click on **New Monitor** link. Choose **DNS Monitor** under **Services** category.
2. Enter the **DisplayName** of the host in which the monitor is running.
3. Enter the **Target Address**.
4. Enter the **Lookup Address**.
5. Enter **Timeout** value in seconds.
6. Select the **Record Type** from the pull down menu.
7. Select the **Search Field** from the drop-down box.
8. Enter **Search Value**.
9. Provide the **Polling interval** for monitoring the DNS monitor.
10. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
11. Associate the monitor instance to the agent.
 1. Enable **Run on Server** option to run the DNS monitor in the local instance of Applications Manager.
 2. Enable **Run on Agent** option to run the DNS monitor from multiple locations. Select the necessary agents from where you want this monitor to be executed. This option will be available only if you enable the EUM add-on.
12. Click **Add Monitor(s)**. This discovers the **Monitor** from the network and starts monitoring them.

FTP/SFTP Monitor

To create an FTP/SFTP Monitor, follow the given steps:

1. Click on **New Monitor** link. Choose **FTP/SFTP** under **Services**.
2. Enter the **Display Name** for the Monitor.
3. Enter the **Target Address** to connect FTP/SFTP.
4. If Authentication is enabled, enter the **Username** and **Password**.
5. Enter **Port No.** (Default port number for FTP is 21 and 22 for SFTP)
6. Enter **Time Out** value.
7. Select the option **YES** or **NO** to indicate whether FTP is secure or not.
8. If you would like to monitor the downloads (mget) through FTP/SFTP while simultaneously downloading the file, select the option **YES** else select **NO**.

9. If the above option is **YES**, then enter the **Remote Src. FileName** (Remote Source FileName) located in the target address.
10. Enter the **Local Dest. FileName** (Local Destination FileName) with full path. The file will download in the given path where the Applications Manager is running.
11. If you would like to upload a file to target address, Select **Upload File** option as **YES** else select **NO**.
12. If YES, enter the **Local Src. FileName** (Local Source FileName) with full path. The file must be available where the Applications Manager is running.
13. Enter the **Remote Dest. FileName** (Remote Destination FileName) with full path where the file will be downloaded in the target address.
14. Provide the **Polling interval** for monitoring the FTP/SFTP monitor.
15. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
16. Click **Add Monitor(s)**. This discovers the **Monitor** from the network and starts monitoring them.

LDAP Monitor

To create an LDAP Monitor, follow the given steps:

1. Click on **New Monitor** link. Choose **LDAP** under **Services**.
2. Enter the **Display Name** for the monitor.
3. Enter the **LDAP Server** and **LDAP Server Port** of the server wherein the services are running.
4. If Authentication is enabled, enter the **Username** and **Password**. If no username and password is provided, then it will connect to LDAP server as anonymous login.
5. Enter the **Searchbase** value.
6. Enter the **Searchfilter** value.
7. Select the **Matching Attribute** from the pull down menu.
8. Select the **Filter Condition** from the pull down menu.
9. Enter the **Search Result** string value which will match with search results.
10. Enter the **Timeout** period which will be used to establish connection with the LDAP server.
11. Click **YES** or **NO** option to check if the connection is secured. If **YES** (to enable SSL mode), then import the certificate of LDAP server into Applications Manager. Please follow the steps (given below) provided to import the LDAP certificate into Applications Manager Truststore.truststore. Once the procedure is complete, restart Applications Manager.
12. Provide the **Polling interval** for monitoring the LDAP monitor.

13. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
14. Click **Add Monitor(s)**. This discovers the **Monitor** from the network and starts monitoring them.

Note: To import certificate into Applications Manager, execute the following command:

```
<Applications_Manager_Home>/working/jre/bin/keytool -import -keystore  
<Applications_Manager_Home>/working/conf/Truststore.truststore -storepass appmanager -  
trustcacerts -alias <alias_name> -file <ldap_certificate_file_path>
```

<Applications_Manager_Home> - Applications Manager installed home directory

<alias_name> - Provide an alias name for the LDAP certificate

<ldap_certificate_file_path> - Provide absolute path to the LDAP certificate

appmanager - This is the password for the LDAP certificate. Ensure that you do not change the password.

See Also

Monitor Information - Services | Create Other New Monitors

Mail Servers

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

- Exchange Server
- Mail Server

Exchange Server

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

1. Click on **New Monitor** link. 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.
6. Select Exchange Server **version** - Exchange 2003, Exchange 2000, Exchange 2007, Exchange 2010, Exchange 5.5.
7. Select the Exchange Server **Services** you want to monitor.
8. Provide the authentication details **User Name\ Domain 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: Monitoring of Exchange Server is possible only if Applications Manager is running in a Windows System. Also, Exchange Server monitor will work only if WMI is enabled in the remote machine in which Exchange Server is running.

Mail Server

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

1. Click on **New Monitor** link. 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.

Web Server / Services

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

- Apache Server
- IIS Server
- Real Browser Monitor (RBM)
- PHP
- SSL Certificate Monitor
- Web Server
- Web Services
- HTTP - URLs and Record & Playback HTTP - URL Sequences

Apache Server

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

1. Click on **New Monitor** link. 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. Enter the **Apache User Name** and **Password** if the Apache Server is **authenticated**.
8. Modify the **Apache Server Status URL** if required. The default Server Status URL through which the data transfer details, access details, etc., are collected is `http://<host-name>:portNumber>server-status?auto`. You can now modify the server status URL using this option, if the server status URL is different.
9. Choose the **Monitor Group** from the combo box with which you want to associate Apache Monitor (optional).
10. 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 on **New Monitor** link. 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.

Real Browser Monitor

Real Browser Monitor (RBM) provides live End-User experience measurement. RBM opens up a Microsoft Internet Explorer Browser and monitors a web application just like how a real user sees it. It supports playback from different geographical locations. To know more about RBM and its monitoring capabilities, see Working of Real Browser Monitor.

Note: Real Browser Monitor supports IE browser only.

To create an Real Browser Monitor, follow the steps given below:

1. Click on **New Monitor** link. Choose **Real Browser Monitor**, under Web Server / Services.
2. Enter the **Display Name** of the RBM
3. Select the **WebScript**, from the available webscripts. To create new webscripts or to modify webscripts, follow the below steps:
 1. Click on *Add/View Webscripts*. It opens up a **Webscript Manager**
 2. Click on *New link*
 3. Enter *New webscript name*
 4. Click on *Record New webscript*
 5. This will prompt you to download the **RBM Toolbar**. Once, you have downloaded the toolbar, a new browser will be opened.
 6. In the browser, you can give the required application URL and go about doing the end user operations.
 7. Click on *stop recording* after the required sequence along with the actions have been recorded.
 8. Save the script in Webscript Manager
 9. For modifying the scripts, select the webscript, do the required changes and save the script.

10. **Note:** Following functions can be added for each URL

1. webCheckText
2. checkElementProperty

webCheckText

Syntax : webCheckText(searchText,prefixText,suffixText)

prefixText and SuffixText are Optional. It checks if the given text is present in the current page. The result of this check will be updated in the details page of the monitor.

Usage :

```
# URL : "http://appmanager/home.html"
setWindowNM("Welcome to ManageEngine Applications Manager","Welcome to
ManageEngine Applications Manager","index",0,1)
webCheckText("Application Manager")
```

checkElementProperty

Syntax:

checkElementProperty(tagName,propertyName,propertyValue,index,propertyNeeded,matchValue)

It checks if a particular element property is present in the current page.

For example in <http://www.appmanager.com> page, I need to check the link Home(Home)

then this function is used to check it.

Usage :

```
# URL : "http://appmanager/home.html"
setWindowNM("Welcome to ManageEngine Applications Manager","Welcome to
ManageEngine Applications Manager","index",0,1)
checkElementProperty("A","href","home.html",1,"target","index")
```

Here the function searches for the element with tagname "A" and the property "href=home.html" . And it checks if the property "target" is equal to "index" . The index denotes the number of occurrences. If the same element is present more than once then we can indicate which element by using index.

4. Select the **Playback Agents**. Multiple selection option is also possible.
 1. Download the **RBMAgent.exe** and install it in remote host/localhost.
 2. Invoke EUM agent through **Start-> All Programs-> ManageEngine EUM agent - > Start Agent** .
 3. While starting EUM agent, configure the Application Manager Host and Port details to add the agent to Application Manager.
5. Set the polling interval time in minutes.
6. Set the **Timeout** in minutes. Timeout is the maximum waiting time taken for the Webscript to execute. If the playback in the EUM agents got struck or was not played back properly, then EUM agent will wait for timeout and then move to the next polling.
7. Click **Add RBM Monitor**.

PHP

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

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

1. Click on **New Monitor** link. 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, ' /phpstats.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.

SSL Certificate Monitor

To create a SSL Certificate Monitor, follow the steps given below:

1. Click on **New Monitor** link. Choose **SSL Certificate Monitor**.
2. Provide an appropriate Display Name for the **SSL Certificate monitor**.
3. Enter the **Domain** name for which SSL certificate is required to be monitored.
4. Provide the **port** in which the server is running [Default port is 443].
5. Check the box **Need proxy to connect to the domain** if the server is connected through proxy. In such cases you should also configure proxy server settings through the 'Configure Proxy' option available in the Admin tab.
6. Enter the **Timeout** value in seconds.
7. Provide the **polling interval** in minutes.
8. Choose the **Monitor Group** from the combo box with which you want to associate the SSL Certificate Monitor (optional).
9. Click **Add Monitor(s)**. This discovers the SSL Certificate from the server and starts monitoring it.

Web Server

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

1. Click on **New Monitor** link. 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.

Web Services

To create Web Services Monitor, follow the steps given below:

Note: If you want to access Web Services through Proxy , Kindly go to Admin > Configure Proxy Settings > Check if Proxy is configured, else configure the same. For hosts that don't require Proxy, add them to the *No Proxy* list.

1. Click on **New Monitor** link. Choose **Web Services**.
2. Enter the **WSDL URL**.
3. Select the checkbox if **proxy** is required for connection to the WSDL URL.
4. Enter the polling interval time in minutes.
5. Enter the **Timeout**.
6. Give the **User Name** and **Password**, if it is required to invoke the webservice operation.
7. Choose the **Monitor Group** from the combo box with which you want to associate Web Services Monitor (optional).
8. Click **Add Monitor(s)**.

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.

After creation of Web Services monitor, you can proceed to add the required **operations** and configure the thresholds and alarms for the same. Kindly refer Web Services Monitor for more details on operations.

See Also

Monitor Information - Web Server / 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 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, 2008, XP, NT, Vista and 7
- Linux
- Sun OS
- IBM AIX
- IBM AS400 / iSeries
- HP Unix
- Tru64 Unix
- FreeBSD
- Mac OS
- Novell

To create any of the above server monitors, follow the steps given below:

1. Click **New Monitor**. 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, AS400 / iSeries, Novell, Linux, HP UX, Sun OS, Windows 2000, 2003, 2008, XP, NT). Based on the type of OS, the 'Mode of Monitoring' information changes.

Windows 2000/2003/2008/XP/NT/Vista:

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.

Note: You have the option to monitor **Windows Event Logs**. Kindly refer Windows Event Log Rules under Admin Operations section.

Linux/Sun OS/IBM AIX/HP Unix/Tru64 Unix/FreeBSD/Mac OS/Novell:

1. Select the Mode of Monitoring (**Telnet**, **SSH** or **SNMP**). For IBM AIX, HP Unix, Tru64 Unix, only **Telnet** and **SSH** are supported. For Novell, only SNMP is supported.
2. If Telnet, provide the port number (default is 23) and user name and password information of the server.
3. If SSH, provide the port number (default is 22) and user name and password information of the server. You also have an option to give Public Key Authentication (User name and Public Key).

Note: To identify the Public/Private key, go to command prompt, type **cd.SSH/** then from the list, open the files `<id_dsa.pub>/<id_rsa.pub>` [Public] or `<id_dsa>/<id_rsa>` [Private] to get the keys.

4. 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`.

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.

IBM AS400 / iSeries:

1. Click on **New Monitor** link.
2. Select **AS400/iSeries**.
3. Enter the **Host Name / IP Address** of AS400/iSeries server.
4. Provide **Subnet Mask** and set **Polling interval** for the monitor.
5. Enter **Username** and **Password** for authentication.
6. Choose the **Monitor Group** from the combo box with which you want to associate AS400/iSeries Monitor (optional).

7. Click **Add Monitor(s)**. This discovers AS400/iSeries from the network and starts monitoring them.

See also: Performance Metrics for AS400 / iSeries

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 only Admin users can log into Windows.

Note: The important configuration details that are required while discovering host resource by Applications Manager are available in Appendix - Data Collection.

Mode of Monitoring - SSH/Telnet vs SNMP

We recommend Telnet or SSH mode of monitoring because the following attributes are not available through SNMP:

- Disk I/O Stats
- Process Monitoring - CPU Utilization
- Swap Memory Utilization

Please check this link for more details.

System administrators generally prefer to check system resources with commands and will prefer to compare it with the SSH/telnet mode output, rather than running SNMP walk to compare. Also, having the connection to the Linux boxes over SSH will make it easier for you to configure the same for script monitors or 'execute program' actions if required.

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(s)-URLs
- HTTP(s)-URL Sequence (Record & Playback)

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.

Note: Get to know how URL monitors can be used for monitoring Response Time across multiple locations - Blog

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**. 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. Multiple keywords should be put within quotes. Otherwise, it will be treated as 'Any' one of the multiple keywords.
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> to <AppMgr Home>\Viblext. Restart Applications Manager.

HTTP-URL Sequence (Record & Playback)

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.

Alarm Mechanism:

Alarms 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 alarm. 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 alarm
- **if response code is:** Select the response code for which alarm 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**. 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.

Note: If you would like to set User Agent for monitoring URL sequence, add the following key in *AMServer.Properties* file located in your Applications Manager installation folder.

am.httpclient.useragent=<Browser User Agent which you would like to set>

Example: **am.httpclient.useragent=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; SV1)**

Save the file and restart Applications Manager for the changes to take effect.

Oracle E-Business Suite

Prerequisites for monitoring Oracle EBS : 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.

Follow the steps given below to create a new Oracle EBS monitor in Applications Manager:

1. Click on **New Monitor**. Click on **Oracle EBS**.
2. Enter Display Name.
3. Provide **Host Name & Port**.
4. Enter the polling interval time in minutes.
5. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
6. Click **Add Monitor(s)**. Upon adding the Oracle EBS monitor, you can view the details of the newly added Oracle monitor.

Please refer Oracle EBS Parameters to know more about the attributes monitored.

See Also

Monitors - Oracle EBS Server Monitor | Create Other New Monitors

SAP Server Monitors

Creating SAP Server Monitor

Prerequisites for monitoring SAP Server : *SAP JavaConnector (JCo)* should be present in Applications Manager's classpath. More

Follow the steps given below to create a SAP server monitor in Applications Manager:

1. Click on **New Monitor**. Click on **SAP Server**.
2. Provide **Host Name / IP Address**.
3. Enter the SubNetMask of the network.
4. Enter the SAP Logon client.
5. Enter the SAP System number.
6. Enter the SAP Logon language like EN for English.
7. Enter the polling interval time in minutes.
8. Enter the **User Name & Password** for SAP.
9. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
10. Click **Add Monitor(s)**. Upon adding the SAP monitor, you can view the details of the newly added SAP monitor.

Kindly refer SAP Parameters to know more about the attributes monitored. Please note that while creating a SAP monitor, you need a SAP user profile with the following authorization objects: S_RFC, S_XMI_LOG and S_XMI_PROD which are minimum prerequisites for adding a SAP monitor.

See Also

Monitors - SAP Server Monitor | Create Other New Monitors

SAP CCMS Monitors

Creating SAP CCMS Monitor

Prerequisites for monitoring SAP CCMS Monitors: *SAP JavaConnector (JCo)* should be present in Applications Manager's classpath. More

Follow the steps given below to add a SAP CCMS monitor in Applications Manager:

1. Click on **New Monitor**. Click on **SAP CCMS** monitor.
2. Enter **Display Name**.
3. Provide **Host Name / IP Address**.
4. Enter the SAP Logon client.
5. Enter the SAP System number.
6. Enter the SAP Logon language like EN for English.
7. Enter the polling interval time in minutes.
8. Enter the **User Name & Password** for SAP server.
9. Select CCMS Monitor Sets by clicking on **Click Here** link. It then displays a list of CCMS monitor sets present in SAP server. Select a CCMS monitor set from the list which you would like to monitor.
10. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
11. Click **Add Monitor(s)**. Upon adding the SAP CCMS monitor, you can view the details of the newly added SAP CCMS monitor.

Kindly refer SAP CCMS Parameters to know more about the attributes monitored. Please note that while creating a SAP monitor, you need a SAP user profile with the following authorization objects: S_RFC, S_XMI_LOG and S_XMI_PROD which are minimum prerequisites for adding a SAP monitor.

See Also

Monitors - SAP Server Monitor | Create Other New Monitors

Virtualization

Server virtualization is one of the highest impact trends in the IT industry today with proven cost savings and other benefits. It is basically a method of running multiple independent virtual operating systems on a single physical computer. It is a way of maximizing physical resources to maximize the investment in hardware.

Applications Manager's monitoring capabilities enables you to ensure your virtual infrastructure is performing as expected.

The following server types supported by Applications Manager under the virtualization category:

- VMware ESX/ESXi
- Microsoft Hyper-V

See Also

[Monitor Information - Virtualization | Create Other New Monitors](#)

 [View Related Blog](#)

VMware ESX/ESXi Servers

Follow the steps given below to create a new VMware ESX/ESXi server monitor:

1. Click on New Monitor link.
2. Select VMware ESX/ESXi under Virtualization category.
3. Specify the Display Name of the VMware ESX server
4. Enter the Host Name or IP Address of the host where the VMware server is running.
5. Enter the Port where the server is running.
6. Enter User Name and Password for authentication.
7. Select the VM Discovery option. The available options are Do not discover, Discover VM but do not monitor metrics, and Discover and Monitor VM metrics.
8. Specify the Polling Interval in minutes.
9. Choose the Monitor Group with which you want to associate the VMware ESX server to, from the combo box (optional).
10. Click Add Monitor(s). This discovers the VMware ESX/ESXi server from the network and starts monitoring it.

User Permissions

In order to add VMWare ESX/ESXi servers for monitoring, we recommend to use the root account. However, in case you are unable to use the root account, you can use a 'view-only' profile to add the servers. This profile has enough rights to be used for monitoring. The user you create must be:

- a member of the group user
- based on the profile 'read only'

Microsoft Hyper-V Servers addon

Follow the steps given below to create a new Microsoft Hyper-V Server monitor:

1. Click the New Monitor drop-down link menu.
2. Select Hyper-V Server under Virtualization category. This action will load the Add Monitor screen.
3. Specify the Display Name of the Hyper-V server.
4. Enter the Host Name or IP Address of the host where the Hyper-V server is running.
5. Enter User Name and Password for authentication.
6. Select the Monitor Performance Metrics of Virtual Machines option if you want Applications Manager to collect performance metrics of VMs of this server.
7. Specify the Polling Interval in minutes.
8. Select the Monitor Group with which you want to associate the Hyper-V server, from the combo box (optional).
9. Click Add Monitor(s). This discovers the Hyper-V server from the network and starts monitoring it.

User Permissions

To monitor a Hyper-V host, the user must have 'Administrator' privileges to the root OS (Windows 2008 R2 and other supported Hyper-V versions).

Firewall Requirements

If a firewall is present between Applications Manager and the Hyper-V server, open ports 135,443 and 1025 in the firewall to enable access.

Amazon Monitors

To create a new Amazon monitor, follow the steps given below:

1. Click on **New Monitor** link.
2. Select **Amazon** under Cloud Apps category.
3. Specify the **Display Name** of the Amazon server
4. Enter the **Access Key Id** of the AWS for accessing the AWS through the API. The access key has 20 alpha-numeric characters.
5. Enter the **Secret Access Key** of the AWS. The secret key should be 40 alpha-numeric characters long.
6. Specify the **Polling Interval** in minutes.
7. Choose the **Monitor Group** with which you want to associate the Amazon monitor to, from the combo box (optional).
8. Click **Add Monitor(s)**. This discovers the Amazon server from the network and starts monitoring it.

Note: Before creating a new Amazon monitor, you have to configure proxy settings under 'Admin' tab.

See Also

Monitor Information - Amazon Monitor | Create Other New Monitors

Custom Monitors

Custom Monitors provide a way to monitor

- Java applications or other applications that expose management information through SNMP (Simple Network Management Protocol) and JMX (Java Management Extensions) - **JMX / SNMP DashBoard**
- File and/or Directory Monitoring - **File / Directory Monitor**
- Windows Performance Counters through generic WMI monitoring - **Windows Performance Counters**
- the output of in-house custom scripts (Windows/Linux) - **Script Monitors**
- Database query monitoring with SQL queries - **Database Query Monitor**

Note: You can also refer to our How-To section on configuring a Custom Monitor.

JMX / SNMP Dashboard

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 Dash Board.

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

1. Select **New Monitor**. 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.

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



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

See Also

Monitors - Custom Monitor | Create Other New Monitors

File / Directory Monitor

To create a file/directory monitor, follow the steps given below:

1. Select **New Monitor**. Choose **File / Directory Monitor**.
2. Provide **Display Name** for the monitor.
3. Select whether it is a **File** monitor or **Directory** monitor.
4. Specify whether the File / Directory to be monitored is in the **Local Server** or **Remote Server**.
5. If it is in the Local server, give the absolute path of the file / directory. If it is in a Remote server, Select the **Host Name** (remote server) from the combo box or you can create a new host (by giving the new host name / IP address, username and password of the host) and the file / directory's absolute path.
6. Enter the string for which you want to check content matching in File. For eg., you can check for exceptions that might occur.
7. Enter the **Polling interval** time period.
8. Choose the **Monitor Group** from the combo box to which you want to associate the Monitor (optional).
9. Click **Add Monitor(s)**. This discovers the file / directory from the network and starts monitoring them.

Important Note:

- File Name / Directory Name should be specified with Absolute Path. (eg) C:\Desktop\test.txt (or) /home/test/test.txt
- In case of Multiple Checks for Content in File Monitoring specify them as comma separated. (eg) NullPointerException,File System Monitor,testString
- Ensure that the file you are monitoring has Read Permission.
- Content Matching in File Monitoring is not supported in Windows Servers.
- To access a Shared Folder, the file path should be given like: \\<hostname>\C\$\Vim
- To monitor a Directory in a remote windows server, ensure that the directory has share permissions, thereby making it available locally. Continue to configure the directory in the local server setup.

See Also

Monitors - File / Directory Monitoring | Create Other New Monitors

Windows Performance Counters

To create windows performance counters in Applications Manager, follow the steps given below:

1. Select **New Monitor**. Choose **Windows Performance Counters**.
2. Provide **Name** for Windows Performance Counter.
3. Enter the **Description** for the counter.
4. Enter the **Polling Interval** for the counter.
5. Select the **Host Name** from the combo box or you can create a new host (by giving the new host name / IP address, username and password of the host)

The windows performance counter values can be added and monitored as attributes. Refer Windows Performance Counters Monitoring to know more about Attributes.

Note: Windows Performance Counters is currently supported for **Windows XP, Windows 2000/2003/2008**.

See Also

Monitors - Windows Performance Counters Monitoring | 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 alarms as per the configuration. Script monitor allows you to monitor the script that is present in the local system or in the remote system, transfers the output to an Output File, parses the output and executes the actions configured.

To add Script Monitor, follow the given steps:

1. Click **New Monitor**. Choose **Script Monitor**.
2. Enter the **Display Name** of the Monitor.
3. Choose whether the script to be monitored is present in the **Local Server** or in a **Remote Server**
4. If it is Local Server, Give the absolute path of the **Script to be Monitored** and also the absolute path of the directory from which the script should be executed. The execution directory should in the same hierarchy of the 'script to be monitored' directory structure.
5. Under Output Settings, Give the **Output file name** with absolute path.
6. Enter the Name of the **String** and **Numeric** attributes.
7. 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.
8. If you want to monitor a tabular Output file, enter the details of the tables - Name, String and Numeric column attributes, delimiter and also specify which attribute is the Unique Column.

Note: Inorder to identify a tabular output file, execute the following commands before and after the actual script.

```
echo<--table <table-name> starts-->
```

```
[Script Commands]
```

```
echo<--table <table-name> ends-->
```

This would enable Applications Manager to identify the Output File's table.

And also, it is mandatory to have the **file headers** as the first line in the file.

9. Specify the **Arguments**. For e.g., hostname 80 http
10. Set the **Polling Interval**. By default, it is 5 minutes
11. Specify the **Timeout** value in seconds. The value can be the maximum time taken by the script to execute.
12. In Linux, Specify the **mode** in which script should be executed. By default, it is "sh".

13. If the script is in a remote server, select the Host Name from the list
14. If the remote server is a new host, then enter the server's **Host Name / IP Address**. Choose the mode of monitoring - **Telnet or SSH**.
15. Enter the **User Name** and **Password** of the server.
16. Enter the **Port** number - Default Telnet port no: 23, SSH: 22
17. Specify the command prompt value, which is the last character in your command prompt. Default value is \$ and possible values are >, #, etc.
18. Upon adding the script monitor, you can view the details of the newly added Script Monitor

Example:

To monitor a script **interfacestatus.bat** that creates a user defined table called **InterfaceStats** and user defined parameters like **DiskStatus**, **DiskErrors** and **No. ofProcess**, in the output file **interfacestatusoutput.txt**

Add Monitor of type Script Monitor

Display Name* Interface Status

Script Location ☒ Local Server ☐ Remote Server

Script to Monitor* c:\interfacestatus.bat

Directory from which the script should be executed* c:\

☒ Output Settings

Output File c:\interfacestatusoutput.txt

String Attributes DiskStatus

Numeric Attributes No.ofProcess
DiskErrors

Delimiter =

☒ Tables in output file

Table Name	Numeric Attributes	String Attributes	Unique Column	Column Delimiter
InterfaceStats	In Out	Name IP	IP	

More Fewer

Arguments (Eg: hostname 80)

Polling Interval * 5 minute(s)

Timeout* 30 second(s)

Associate Monitor Instance to Monitor Group

Select the Monitor Group -- Select Monitor Group --

Add Monitor(s) Restore Defaults Cancel

Outputfile Sample: interfacestatusoutput.txt

```

<--table InterfaceStats starts-->
Name IP Status In Out
IF1 192.168.112.210 up 234 435
IF2 192.168.112.212 up 434 122
IF3 192.168.112.214 down 434 122
<--table InterfaceStats ends-->

DiskStatus = ok
DiskErrors = 4
No.ofProcess = 60

```

In the Script Monitor creation form, give the **absolute path of the script** : **c:\interfacestatus.bat**

Output settings:

Give the absolute path of Output file: `c:\interfacestatusoutput.txt`

Give *DiskStatus* as the string attribute, *No.ofProcess* and *DiskErrors* are the numeric attributes with *Delimiter* "="

If you want to monitor statistics in a table format , select Tables in output file.

Here, we have the table *InterfaceStats* with the stats Name, IP, Status, In, Out where Name, IP, Status are string attributes; In & Out are numeric attributes. The *Delimiter* is the separator between the two column names -> space. If tab is the delimiter, then give `\t` . Usually tab will be the delimiter for sql queries results.

Note: The starting tag of the table, *InterfaceStats* is "`<--table InterfaceStats starts-->`" and the end tag is "`<--table InterfaceStats ends-->`". Also, the first line of the table should contain the attribute names. The attribute names or the column names should also be separated by the same delimiter used to separate the data rows and that is specified as the column delimiter. In this case, they are Name, IP, Status, In and out. The remaining lines between the start and end tag should comprise of the actual data. Make sure that the delimiter for the table is unique and you should specify that as the column delimiter.

Unique Column is the attribute that doesn't repeat itself in the rows and identify the row by that value. Here it is *IP*.

See Also

Monitor Information - Script Monitors | Create Other New Monitors

Database Query Monitor

Database Query Monitor is used to monitor a single query or a set of queries for any given database. This SQL based query monitor allows user to monitor the status of that particular query.

To add Database Query Monitor, follow the given steps:

1. Click **New Monitor**. Choose **Database Query Monitor**.
2. Enter the **Display Name** of the Monitor.
3. Enter the **Host Name** of the Monitor on which the database is running.
4. Enter the **Port number**.
5. Select the **DB** type for which the query is being executed.
6. Enter the **Username and Password** of the database server.
7. Enter the **Database name**.
8. Select whether you would prefer **Query Output** by choosing the **Yes** or **No** radio button.
9. Enter the **Query**. Please note that the number of queries is limited to five queries. Also, note that the delimiter for a query is new line.
10. Enter the **Polling Interval**. By default, it is 5 minutes.
11. Choose the **Monitor Group** from the combo box with which you want to associate Database Query monitor.

See Also

Create Other New Monitors

J2EE Web Transaction Monitor

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

Prerequisite: J2EE 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 **J2EE Web Transaction monitor**:

- Click **New Monitor**. Choose **J2EE 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 J2EE 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 J2EE Web Transaction Monitor supports **JDK1.5** and above.

See Also

Monitor Information - J2EE Web Transactions Monitor | Create Other New Monitors

Java Runtime Monitor

Java Runtime Monitor provides out-of-the-box remote monitoring and management on the Java platform and of applications that run on it.

The different JVM vendors supported by Applications Manager are Sun JVM, IBM JVM and Oracle JRockit JVM.

PreRequisite: To monitor JDK1.5 JVM and above, the following java runtime options need to be added to your application start up file.

-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=1099 -

Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false

Note : Port number "1099" can be replaced with the actual port number of the JMX agent.

Also **Note:** Support is available for JRE1.5 and above

Example: To enable Java Runtime Monitor in JBoss do the following

Edit the *run.sh/bat* under JBoss *home/bin*. Append the following command to JAVA_OPTS

```
JAVA_OPTS =-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=1099 -
```

```
Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false
```

```
%JAVA_OPTS%
```

To enable Java Runtime Monitor in Tomcat do the following

Edit the *run.sh/bat* under Tomcat *home/bin*. Append the following command to JAVA_OPTS

```
JAVA_OPTS =-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=1099 -
```

```
Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false
```

```
%JAVA_OPTS%
```

Follow the steps given below to create a **Java Runtime Monitor**:

- Click **New Monitor**. Choose **Java Runtime**.
- Enter the **IP Address or hostname** of the host in which the Monitor is running.
- Enter the SubNetMask of the network.
- Provide the **port number** in which JDK is running (default: 1099). Also, you can provide multiple ports separated by commas.
- Enter the polling interval time in minutes.
- Enter the **JNDI name**. For example, */jmxrmi*.
- If Authentication is enabled, enter the Username and password.
- Choose the **Monitor Group**, to which you want to associate the Monitor (optional).
- Click **Add Monitor(s)**. This discovers the Monitors from the network and starts monitoring them.

See Also

Monitor Information - Java Runtime Monitor | Create Other New Monitors

Custom Monitor Type

By using this option, you can define your **own monitor types** apart from the monitor types that are available by default.

This feature allows to associate a monitor type to the inhouse scripts that might be used for monitoring your own applications. For eg., if you are using various scripts to monitor Siebel CRM, you can now associate these scripts and model Siebel as one of the monitor types. Thereby having robust out of the box support for monitoring Forum Software, build Business Intelligence Dashboards, monitor Custom Application Log Files on multiple servers etc.

Custom Monitor Demo: Have a look at the demo that helps you to add a new Custom Monitor Type

WorkFlow

Step1) The custom monitor type helps you create and define *metrics / attributes* that will be tracked.

Step 2) Then specify a script (Linux Shell Script / Windows Batch File) that needs to be executed to get the data and provide it to Applications Manager in the appropriate format.

In these scripts users can use any mechanism to get the data. For example users can :

- Invoke a Java Program, PHP, Python Scripts etc and make database calls to pull data and feed it to Applications Manager
- Can make native calls to other programs and pipe the data to the output file
- Parse Log Files and give a summary of metrics as the input to Applications Manager

Creating New Monitor Types:

You can create new monitor type by clicking on the '*New Monitor Type*' link inside the *New Monitor* link or by clicking on the *Custom Monitor Types icon* under *Admin* tab.

- Enter the *Monitor Type* name
- Select Base type - Currently, scripts are the base to build new monitor type.
- Select the Monitor Type *Category* - For eg., If you are monitoring postgresql using in-house scripts, you can add postgresql monitor type and you can place it under Database category

Define the **attributes** you want to monitor

- Enter the String Attributes that you want to monitor - Enter the attributes line by line.
- Enter the Numeric Attributes that you want to monitor - Enter the attributes line by line.
- You can monitor the output in a *table format*, enter the Table Name, Numeric attributes, Sting attributes, Unique column and Column delimiter. More help
- Click on *Create Monitor Type* to finish the configuration of new monitor type.

Now, you have defined a custom Monitor type. The next step would be to create instances & associate them to the new monitor type defined.

[Script Monitor Overview: Based on the polling interval, Applications Manager executes the script to be monitored. The script will transfer its output to another specific *Output File* configured. The output of the script should be in a Key=Value format where '=' can be any delimiter. Applications Manager parses the Output File and executes the actions configured]

Adding Custom Monitors:

- In the *User Created Monitor Type* screen, the newly created monitor types are listed down. Click on the *Add New* icon to add the monitors
- Add New monitor screen opens up, Select the custom monitor type from Monitor Types drop down box. [For eg., Siebel]
 - Enter the Display Name.
 - Choose the location of script that you want to monitor - Local or Remote.
 - Specify the absolute path of the script.
 - Specify the absolute path of the execution directory.
 - Specify the absolute path of the Output File
 - Enter the arguments that needs to be passed.
 - Enter the polling interval and timeout.
 - Click Add Monitor(s)

You have already given the attributes to be monitored as common to all monitors under custom Monitor Type. So there is no need to give input attributes to be monitored again

- Upon adding the custom monitors, you can see the performance attributes in the monitor details page.

Usage Scenario 1: Creating New Siebel Monitor Type

One customer had 6 Siebel applications running in 6 different machines. As, out of the box support for Siebel Application is not available, he uses the Script Monitoring feature of ManageEngine Applications Manager to monitor his applications. He has identical scripts running in the 6 machines and they produce the same output in the output file in the respective machines. Now he configures them as six Script Monitors. This gives him an opportunity to monitor his Siebel applications. Using Script Monitor facility, he monitors the following attributes

- transaction Router
- server request processor
- transaction processor

There are few disadvantages in his usage.

1. He has to give the same Output details while specifying the same six applications.
2. If he has to edit / add / delete the attributes , then he has to do so in all the 6 Script Monitors.
3. Further he would like to see them as 6 Siebel Monitors rather than 6 Script Monitors.

Here comes the usage of New Monitor Type, that would avoid all the above inconveniences.

1. Output Settings can be specified only once. You could specify the Scalar String / Numeric attributes and tabular settings only once while defining the type, say Siebel.

2. You could create any number of monitor instances for that particular type , just like any other in-built type say SAP / Weblogic / Oracle monitors in Applications Manager. While doing so, you just need to specify the Hostname and the corresponding Scripts
 3. Adding / Deleting / Modifying attributes of some particular monitor type commonly will affect all the monitors of that monitor type.
 4. Now you will be seeing 6 Siebel monitors rather than 6 Script Monitors.
 5. Reports can be enabled for this type like any other type.
- The same concept can be applied to any other application say for monitoring People Soft applications.

Usage Scenario 2: Business Intelligence Dashboard

Users can build custom **Business Intelligence dashboards** and have it reported and alerted on. Some possible metrics could be

- Call Volume in the last one Month
- Time taken to finish a call
- Number of simultaneous Calls

Usage Scenario 3: Custom Application Log Files

Some metrics that you can add with a little bit of coding are :

- Number of security breaches
- Number of Errors During Login etc.

Managing Custom Monitor Types:

You can edit the configuration of the Monitor types by clicking on the **Custom Monitor Type** link under **Admin Tab**. It opens up to list all the User created Monitor Types. From here you add new monitors to the custom monitor types, edit the configuration and more importantly **enable or disable reports** of these custom monitor types.

Viewing Performance Metrics

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.

Monitor Types

Applications Manager supports the following Monitor Types:

1. Application Servers
 - Microsoft .NET
 - JBoss Servers
 - GlassFish Servers
 - Oracle Application Servers
 - SilverStream
 - Tomcat Servers
 - VMware vFabric tc Servers
 - WebLogic Servers
 - WebSphere Servers
2. Database Servers
 - MySQL Database Servers
 - Oracle Database Servers
 - MS SQL Database Servers
 - IBM DB2 Database Servers
 - Sybase Database Servers
 - PostgreSQL Database Servers
 - Memcached Database Servers
3. Middleware / Portal Monitors
 - Microsoft Message Queue (MSMQ)
 - WebLogic Integration Servers

- Microsoft Office Sharepoint Server
- IBM WebSphere MQ

4. Servers

- Windows
- Linux
- Solaris
- IBM AIX
- IBM AS400 / iSeries
- HP Unix
- Tru64 Unix
- Free BSD
- Mac OS
- Novell

5. Services

- JMX Applications
- Ping Monitor
- Service Monitoring
- AdventNet JMX Agent
- SNMP / Network Device
- Telnet
- Active Directory
- DNS Monitor
- FTP / SFTP Monitor
- LDAP Monitor

6. Mail Servers

- Exchange Server
- Mail Server

7. Web Server / Services

- Apache Server
- IIS Server
- Real Browser Monitor
- PHP

- Web Services
- Web Server
- HTTP(s) URL Monitors and HTTP(s) URL Sequence (Record & Playback)

8. ERP

- SAP
- SAP CCMS
- Oracle E-Business Suite

9. Virtualization

- VMware ESX/ESXi servers
- Microsoft Hyper-V Servers
- Virtual Machines

10. Custom Monitors

- JMX / SNMP Dashboard
- File System Monitor
- Windows Performance Counters
- Script Monitor
- Database Query Monitor

11. Java / Transaction Monitors

- Java Runtime Monitor
- J2EE Web Transactions

12. Network Monitoring Connector

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
- GlassFish Servers
- JBoss Servers
- Oracle Application Servers
- SilverStream
- Tomcat Servers
- VMware vFabric tc Server
- 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. Data collection happens through WMI. 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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Availability	Shows the current status of the .Net - available or not available.
Threads Physical Threads Logical Threads	Shows the number of native OS threads created & owned by the CLR to act as underlying threads for .NET thread objects. Shows the number of current .NET thread objects in the application.
Memory Heap Size % Time in GC	Shows the current memory allocated (MB) 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
Locks Queue Length Contentions/Min	Refers to the total number of threads currently waiting. Refers to the rate at which threads in the runtime attempt to acquire a managed lock unsuccessfully.
Exceptions Exceptions/Min	Refers to the number of exceptions per Minute
Security TotalRuntimeChecks/Min	Refers to the total number of runtime Code Access Security (CAS) checks performed per minute.
JIT % Time In JIT	Refers to the percentage of elapsed time spent in JIT compilation since the last JIT compilation phase.

.NET Applications Details	Clicking on the Names of the .NET applications, you can see their performance based on their parameters.
----------------------------------	--

The various .NET application's parameters that are monitored are:

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

See Also

Creating New Monitor - Microsoft .NET

GlassFish Servers

Monitored Parameters

GlassFish servers are monitored based on the attributes such as memory, thread, etc. The monitoring details of GlassFish 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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Name	The Name of the Server
Availability	Shows the current status of the server - available or not available.
Last Polled at	Specifies the time when the monitoring of the server was recently done
Next Poll at	Specifies the next polling time for monitoring the server
Response Time	Refers to time required for the Glass Fish server to respond while monitoring
Memory Details	
Used Memory	Refers to JVM heap used in KB
Total Memory	Refers to the JVM total heap size
Thread Details	
Thread Count	Total number of Threads in JVM in which GlassFish is running
Running	Refers to the state of totals thread that are in runnable state in the JVM
Waiting	Refers to the total no. of threads that are waiting for a monitor lock in the JVM
Blocking	Refers to no. of total threads that are blocked waiting for a monitor lock
Deadlocked	Refers to the no. of total threads that are blocked forever in the JVM
Timed Waiting	Refers the total threads that are waiting for another thread to perform an action for up to a specified waiting time

Parameter	Description
Table WebApp Monitoring	
Name	Name of the Web Application
Session High Count	Maximum number of concurrently active sessions
Session Current Count	List of currently active sessions in the Web Application
Total Sessions Rejected	Total number of rejected sessions

See Also

Creating New Monitor - GlassFish Server

JBoss Servers

Supported Versions

Applications Manager supports monitoring of JBoss Servers of versions 3.2.x, 4.0.x, 4.2.2 GA, 5, 5.1. Performance data is collected by deploying an agent automatically from Applications Manager to the JBoss server that needs to be monitored.

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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
JBoss Version	The version of the JBoss Server.
Listen Port	The port at which the JBoss server listens.
Web Server Port	The port at which web server service is running.
Activation Time	Specifies the time when the JBoss Server was started.
Monitoring Started Time	Specifies the time when the monitoring of the server was started.
Availability	Shows the current status of the server - available or not available.
JVM Usage	Refers to the current amount of free and used memory in the JVM heap in kilobytes.
Server Response Time	Refers to the time required for the server to respond while monitoring.
Web Applications Details	
Name	Name of the Web Application
Context Root	Specifies a context root of the Web application.
Response Type	Lists the different HTTP status code that are obtained for every request sent to web applications.

Parameter	Description
Total Number of Requests	The number of requests for each response types.
Average requests per Data Collection Cycle	The average requests processed for every data collection cycle.
Servlet Details	
Name	Specifies the name of the servlet.
Execution Time	Specifies the total execution time, in milliseconds, for the servlet.
Invocation Count	Specifies the number of times that the servlet is invoked, i.e. the hits of the Servlet.
Enterprise Java Bean Details	
Name	Name of the EJB
Type	Type of the EJB - Entity Bean, Stateless Session Bean, Stateful Session Bean, and Message Driven Bean.
Module	Refers to the jar to which the EJB belongs.
Number of Instances Created	Specifies the total number of EJB instances created.
Number of Instance Removed	Specifies the total number of EJB instances destroyed.
Number of Instances Available for Processing	Specifies the total number of EJB instances that are available for processing requests.
Number of Instances in ready state	Specifies the total number of EJB instances that are in ready state.
Number of Instances in Pooled state	Specifies the total number of EJB instances that are in pooled state.
JDBC Connection Pool Details	
JDBC Pool	Name of the Connection Pool.
Pool Size	Number of connections in the pool.
Connections Currently in Use	Number of connections that are currently being used.
Connections created	Total number of connections that have been created after the pool was instantiated.

Parameter	Description
Connections destroyed	Total number of connections that have been destroyed after the pool was instantiated.
Idle Time Out (Mins)	Maximum number of minutes that an idle (unallocated) connection can remain in the pool before being removed to free resources.

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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Port	The port at which the Oracle Application server listens.
Last Polled at	Specifies the time when the monitoring of the server was started.
Availability	Shows the current status of the server - available or not available.
Request Throughput	
Throughput	Number of requests processed per unit of time in the server.
Current Active Connection	Shows the current active connections
Average Connection Process Time	Gives the average processing time of the connections
Current Active Request	Shows the number of requests that are active currently
Server Response Time	
Response Time	Refers to the time required for the server to respond while monitoring.
Data Throughput	Refers to how much data is transferred per unit time
Data Processed	Refers to how much data is processed per request

Parameter	Description
Servlets	Total number of servlets
OPMN Process Memory Stats (Memory statistics of the OPMN processes like dcm-daemon, WebCache, WebCache Admin, HTTP_Server, home)	
Used Memory	Gives the total physical memory used by the process
Status	Gives the availability status of the process
oc4j JVM Statistics	
Active Thread Groups	Shows the number of Active Thread groups in the JVM
Active Threads	Shows the number of Active Threads in the JVM
Heap Usage	Shows current heap memory usage of the process
JDBC Connections	Gives the total number of JDBC Connections
Transactions	Gives the total number of open, committed and aborted JDBC transactions
Web Applications	
Servlets	Total number of servlets in the web application
Throughput	Number of requests processed per unit of time in the web application
Process Request	Time taken to process the request
Active Request	Current number of active requests for the web application
Active Session	Number of active sessions of the web application
Session time	Total time for which the sessions have been active
JMS Attributes	
Deque Avg	Average time to deque messages
Enque Avg	Average time to enque messages
Pending Message	Total number of message waiting to be processed
Message Dequeued	Total number of messages dequeued
Message Enqueued	Total number of messages enqueued

Parameter	Description
Message Count	Number of messages in the JMS Destination
EJB Statistics	
EAR Name	Name of the Enterprise Application Resource
Process	Name of the oc4j process to which the EJB belongs to
Type	Gives the type of the EJB
Create Count	Number of EJBs created
Active Count	Number of active EJBs
Passive Count	Number of passive EJBs
Pooled Count	Number of pooled EJBs
Response Summary	Gives the count for the various HTTP responses

See Also

Creating New Monitor - Oracle Application Server

SilverStream Servers

Monitored Parameters

SilverStream servers are monitored based on the attributes such as memory, thread, etc. The monitoring details of SilverStream 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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Name	The name of the server
Health	The health of the server
Availability	The availability status of the server
Last Polled at	The time at which last poll happened
Next Poll at	The time at which next poll has been scheduled
Memory Details	
Free Memory	Available Memory in MB for the JVM
Total Memory	Total Memory used by JVM
GC Count	No. of time Garbage Collection happened
Request Details	
Minimum Response Time	The least time taken to process a request
Average Response Time	Average time taken to process a request
Maximum Response Time	The maximum time taken to process a request
Thread Details	
Free Threads	No. of free threads
Idle Threads	No. of threads that are waiting for a task

Total Threads	Total number of threads available
Load Details	
Requests	No.of requests processed by the server
Current Load	Load on the SilverStream Server
Bytes	No. of bytes transferred by the server
Session Details	
Idle Sessions	No.of sessions in idle state
Total Sessions	Total number of sessions
License Details	
Used Licenses	Total number of licenses used
Total Licenses	Total number of licenses available

See Also

Creating New Monitor - SilverStream 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 and above

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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

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

Parameters	Description
Session Details	Gives the number of sessions of the Tomcat Server.

The data displayed differs between each version of the Tomcat Server. For Tomcat Server 3.x and 4.x, agent has to be deployed for monitoring.

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

Data displayed for Tomcat 5.x and above

1. Availability
2. Response Time Details
3. Memory Usage
4. Thread Details
5. Response Summary
6. Application Summary and Details.
7. Session 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.x
5. WebLogic 10.x

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 alarms based on the thresholds configured on the numerical attributes of the server.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameters	Description
Monitor Details	
WebLogic Version	Refers to the version of the WebLogic Server.
State	Refers to the server state such as running and down.
Listen Port	Specifies the port at which the WebLogic Server listens for connections.
Activation Time	Specifies the time when the WebLogic Server was started.
Availability	Shows the current status of the server - available or not available.
JVM Heap Size	Refers to the current size of the JVM heap in kilobytes.
Server Response Time	Refers to the time required for the server to respond while monitoring.
Web Application Details	
Name	Name of the Web Application.

Parameters	Description
Number of Active Sessions	Specifies the number of sessions that are currently active in the Application.
Maximum Number of Sessions	Refers to the highest number of sessions that were open for an Application.
Total Number of Sessions	Refers to the total number of sessions that were opened since deployment of an Application.
Number of Servlets	Refers to the total number of servlets of a web application. Click on the number, to find details on Servlets as explained below.
Servlet Details	
Name	Specifies the name of the servlet.
Execution Time	Specifies the total execution time, in milliseconds, for the servlet.
Invocation Count	Specifies the number of times that the servlet is invoked, i.e. the hits of the Servlet.
Enterprise Java Bean Details	
Name	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.
Type	Specifies the bean type - Entity, Stateless Session, Stateful Session, and Message Driven beans
Activation Count	Refers to the total number of beans activated (i.e. from the Secondary storage to Primary storage) for that particular Bean container.
Passivation Count	Refers to the total number of beans passivated (i.e. from the Primary storage to Secondary storage) for that particular Bean container.
Threads Waiting	Specifies the total count of idle threads assigned in the thread queue.
Cached Beans Current Count	Refers to the number of Cached Beans in the container.
Beans In Use Count	Specifies the number of beans currently in use.
Idle Beans Count	Specifies the number of beans that are currently idle.
Transaction Timed Out Count	Specifies the total number of transactions, which have been rolled back due to timeout.

Parameters	Description
Transaction Rolled Back Count	Refers to the total number of transactions that are rolled back.
Transaction Committed Count	Refers to the number of transactions committed or completed successfully.
Database Connection Pools Details	
Name	Name of the database connection pools that enables caching of database connection in the monitor easier through pools.
Connection Pool Size	Specifies the number of database connection pool.
Active Connections	Mentions the number of active connections made to the monitor.
Leaked Connections	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.
Thread Waiting	Mentions the number of threads waiting for the connection.
Thread Pools Details	
Name	Name of the thread pools.
Total Threads	Refers to the total count of threads assigned in this thread queue.
Idle Threads	Specifies the threads that are idle or not used.
Threads In Use	Specifies the threads that are currently in use.
Pending Requests Count	Specifies the number of requests that are pending in the queue.
SAF Details	
Name	Name of SAF Agent in Weblogic
Conversations Current Count	The current number of conversations
Conversations Total Count	The total number of conversations since the last reset
Remote Endpoints Current Count	The current number of remote endpoints to which this SAF agent has been storing and forwarding messages.

Parameters	Description
Remote EndpointsTotal Count	The number of remote endpoints to which this SAF agent has been storing and forwarding messages per minute
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 versions of the WebSphere Servers can be monitored by Applications Manager:

- WebSphere 5.x, 6.x, 7.x and above

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. List view enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information

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.

Parameters	Description
Monitor Details	
WebSphere Version	Denotes the version of the WebSphere server monitor.
State	Refers to different states of the Websphere server such as running and down.
HTTP Port	Refers to HTTP Transport port.
Transaction Details	Specifies Global Commit Duration, Committed Transactions, Transactions Rolled Back and Transactions Optimized.
Server Response Time	Specifies Minimum, Maximum, Average and Current Response Time.
Availability	Specifies the status of the WebSphere server - available or not available.
JVM Memory Usage	Specifies the total memory in JVM run time.
CPU Utilization	Specifies the average system CPU utilization taken over the time interval since the last reading.
Free Memory	Specifies the amount of real free memory available on the system.
Average CPU Utilization	Specifies the average percent CPU Usage that is busy after the server is started
Session Details of Web Applications	
User Sessions	Specifies the total number of sessions that were created.

Parameters	Description
Invalidated Sessions	Specifies the total number of sessions that were invalidated.
Affinity Breaks	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.
EJB Details	
Name	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.
Type	Denotes the different types of the bean such as entity, stateless session, stateful session, and message driven.
Concurrent Lives	Specifies the number of concurrent live beans.
Total Method Calls	Specifies the total number of method calls.
Average Method Response Time	Specifies the average time required to respond to the method calls.
Pool Size	Specifies the number of objects in the pool (entity and stateless).
Activation Time	Specifies the average time in milliseconds that the total bean is activated for that particular Bean container, including the time at the database, if any.
Passivation Time	Specifies the average time in milliseconds that the total bean is passivated for that particular Bean container, including the time at the database, if any
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.

Parameters	Description
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.

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 Troubleshooting tips](#)(opens in new window)

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 alarms, 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
- Sybase Database Servers
- PostgreSQL Database Servers
- Memcached Database Servers

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

For all databases, data collection happens by establishing a JDBC connection and executing queries to collect the data.

See Also

Creating New Monitor - Database Server

MySQL DB Servers

Supported Versions

- MySQL 3.23.x
- MySQL 4.x, 5.x

Monitored Parameters

The *Availability* tab gives the Availability history for the past 24 hours or 30 days. The *Performance* tab gives the health status and events for the past 24 hours or 30 days. The *List view* enables you to perform bulk admin configurations.

To view detailed performance metrics of a MySQL server, click the corresponding monitor listed in the *Availability* tab. These metrics are categorized into two different tabs for better understanding.

Overview

This tab provides information into the overall performance of the MySQL server.

Parameter	Description
Monitor Information	
Name	Denotes the name of MySQL server monitor.
Health	Denotes the health (Clear, Warning, Critical) of the MySQL server.
Type	Denotes the type you are monitoring.
MySQL Version	Specifies the version of the database server.
Port	Specifies the port number at which the database server is running.
Base Directory	Specifies the directory in which the database server is installed.
Data Directory	Specifies the directory in the hard disk of the system where the data for the database server is stored.
Host Name	Specifies the host at which the database server is running.
Host OS	Specifies the OS of the host where the database server is running.
Last Alarm	Specifies the last alarm that was generated for the database server.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.
Connection Time	
Connection Time	Specifies the time taken to connect to the database
Connection Time Out	Specifies the maximum time taken by the application to connect to MySQL Server
Request Statistics	
Request Rate	Number of request received in one second.

Parameter	Description
Bytes Received Rate	Number of bytes received in one second.
Bytes Sent Rate	Number of bytes sent in one second.
Connection Statistics	
Open Connections	The number of connections opened at present in the MySQL Server.
Aborted Connections	Number of tries to connect to the MySQL server that failed.
Aborted Clients	Number of clients aborted by MySQL server.
Thread Details	
Threads Used	Number of threads processing the request.
Threads in Cache	Number of threads currently placed in the thread cache.
Thread Cache Size	Specifies the cache size in the MySQL server.
Database Details	
Database Name	Name of the database instance.
Database Size	Size of the various databases in the MySQL server.
Table Lock Statistics	
Immediate Locks	Number of times a table lock for the table is acquired immediately.
Locks Wait	Number of times a table lock could not be acquired after waiting.
Key Efficiency	
Key Hitrate	Percentage of key read requests that resulted in actual key reads from the key buffer.
Key Buffer Used	Amount of allocated key buffer in use.
Key Buffer Size	Size of the buffer used for index blocks. Also known as the key cache.
Query Statistics	
Queries Inserted/Min	No. of Insert Queries executed per minute
Queries Deleted/Min	No. of Delete Queries executed per minute
Queries Updated/Min	No. of Update Queries executed per minute

Parameter	Description
Queries Selected/Min	No. of Select Queries executed per minute
Query Cache Hitrate (This performance data is not available for MySQL versions 3.23.x)	
Query Cache Hitrate	Ratio of queries that were cached and queries that were not cached.
Query Cache Size	Amount of memory allocated for caching query results.
Query Cache Limit	Maximum amount of memory for storing cache results.
Replication Details	
Replication Status	The status of Slave process in MySQL Server
Slave IO Running	Status of the Slave IO Process in MySQL Server. Possible values are Yes/No
Slave SQL Running	Status of the Slave SQL Process in MySQL Server. Possible values are Yes/N.
Last Error	The last error occurred when Slave is synching the data from master.
Master Host	The hostname or IP number of the master replication server.
Master Port	The TCP/IP port number that the master is listening on
Master User	The username of the account that the slave thread uses for authentication when it connects to the master
Time Behind Master	This indicates of how "late" the slave is behind the Master

Configuration

This tab provides information about the system variables maintained by the MySQL server. These system variables indicate how the server is configured.

You can also view realtime and historical data of any of the attributes present in the 'Configuration Information' section in the Configuration tab. Click on any attribute under the Configuration tab. This will open up a new window named 'History Data' that provides more information about these attributes.

There are two tabs in the History Data window - History Report and Global View.

History Report: This tab provides historical reports of the attribute selected based on the time period chosen. You can also use the *Select Attribute* drop-down box and view reports for other attributes.

Global View: This tab displays the current values of the attribute selected, across multiple monitors. To view information about other attributes present in the monitor, use the *Select Attribute* drop-down box and change the attribute.

If you want to view data of multiple attributes, click the *Customize Columns* link present at the top left corner of the window. This will take you to the *Edit Global View* screen. In this screen, you can change the monitor type using the *Filter by Monitor Type* drop-down box, select the metrics to be displayed, and show monitors on a monitor basis or a monitor group basis. After you select your options, click the *Show Report* button to view those information in the Global View tab.

The **View Process List** option present on the right side under the *Show Status* section gives you information on the current threads that are running in the MySQL server.

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, 10.1.3, 11g, RAC (*Real Application Clusters*)

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Note: For you to create a new Oracle database monitor, you should have admin privileges. Minimum User Privileges -> user with CONNECT and SELECT_CATALOG_ROLE roles

Monitor Information

Parameters	Description
Name	Name of the Oracle server monitor
Oracle Version	Refers to the Version of the Oracle Database.
Oracle Start Time	Refers to the time when Oracle server was started.
Availability	Refers to the status of the database server - available or not available.

Connection Time

Parameters	Description
Connection Time	Refers to the time taken to connect to the database.

User Activity

Parameters	Description
Number of Users	This refers to the number of users executing an SQL Statement.

Database Details

Parameters	Description
Database Created Time	Creation time of the database.
Open Mode	Indicates the Open mode of the Instance which can be either Read Write or Read .
Log Mode	If the transactions are written on the Log, the Log mode will be ARCHIVELOG , or else, the Log mode will be NOARCHIVELOG.

Database Status

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

Table Space Details

Parameters	Description
Name	Refers to the name of the Table space.
Allocated Bytes	Refers to the size of the Table space in bytes.
Allocated Blocks	Refers to the number of allocated blocks in Table space.
Data Files	Refers to the number of data files in Table space.

Table Space Status

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

SGA Details

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

SGA Status

Parameters	Description
Buffer Hit Ratio	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.

Parameters	Description
Data Dictionary Hit Ratio	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.
Library Hit Ratio	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.
Free Memory	Refers to the size of the free memory in bytes.

Performance of Data Files

Parameters	Description
Data File Name	Name and location of the data file.
Table Space Name	Name of the Table space.
Status	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.
Created Bytes	Size of the Data file in bytes.
Reads	Refers to the number of reads from the Data file.
Writes	Refers to the number of writes to the Data file.
Average Read Time	Refers to the average read time.
Average Write Time	Refers to the average write time.

Session Details

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

Rollback Segment

Parameters	Description
Segment Name	Name of the rollback segment.
Table Space Name	Name of the tablespace containing the rollback segment.
Status	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.
Current Size	Current size in bytes of the rollback segment.

Parameters	Description
Initial Extent	Initial extent size in bytes.
Next Extent	Secondary extent size in bytes.
Min. Extent	Minimum number of extents.
Max. Extent	Maximum number of extents.
Hit Ratio	Ratio of gets to waits . This should be $\geq 99\%$.
HWMSize	High Water Mark of rollback segment size.
Shrinks	Number of times rollback segment shrank, eliminating one or more additional extents each time.
Wraps	Number of times rollback segment wraps from one extent to another.
Extend	Number of times rollback segment was extended to have a new extent.

Session Waits

Parameters	Description
ID	Session Identifier for the connected session.
User Name	Name of the Oracle process user.
Event	Resource or event for which the session is waiting
State	Wait state: 0 - WAITING (the session is currently waiting) -2 - WAITED UNKNOWN TIME (duration of last wait is unknown) -1 - WAITED SHORT TIME (last wait $< 1/100$ th of a second) >0 - WAITED KNOWN TIME (WAIT_TIME = duration of last wait)
Wait Time	A nonzero value is the session's last wait time. A zero value means the session is currently waiting.
Seconds in Wait	If WAIT_TIME = 0, then SECONDS_IN_WAIT is the seconds spent in the current wait condition. If WAIT_TIME $\neq 0$, then SECONDS_IN_WAIT is the seconds since the start of the last wait, and SECONDS_IN_WAIT - WAIT_TIME / 100 is the active seconds since the last wait ended.

Note: By default the below attributes are not monitored, but to monitor these metrics, go to Admin tab -> Performance Datacollection -> Oracle -> Enable **Top 10 Queries by Disk Reads and Buffer Gets, Lock and Wait Statistics**

Buffer Gets

Parameters	Description
Buffer Gets	Number of buffer gets for the child cursor
Executions	Number of executions that took place on the object since it was brought into the library cache
Buffer Gets per Executions	The ratio of buffer gets to execution in the current polling interval
Query	First thousand characters of the SQL text for the current cursor

Disk Reads

Parameters	Description
Disk Reads	Number of disk reads for this child cursor
Executions	Number of executions that took place on this object since it was brought into the library cache
Disk Reads per Executions	The ratio of disk reads to execution in the current polling interval
Query	First thousand characters of the SQL text for the current cursor

DBABLOCKERS

Parameters	Description
Id	Session identifier of Session holding a lock
Serial	Session serial number. Used to uniquely identify a session's objects. Guarantees that session-level commands are applied to the correct session objects if the session ends and another session begins with the same session ID.
Machine	Operating system machine nam
PROGRAM	Operating system program name
Lock Wait	Address of lock waiting for; null if none

DBAWAITERS

Parameters	Description
Waiting Session ID	ID of Session waiting for lock
Holding Session ID	ID of Session holding lock
Lock Type	The lock type
Mode Held	The mode held
Mode Requested	The mode requested
Lock ID1, ID2	The Lock IDs

Lock Statistics

Parameters	Description
Object Name	Name of the locked object
Session Id	Session Id of locked object
Serial	Session serial number. Used to uniquely identify a session's objects.
Lock Mode	Mode of lock
OS Process ID	Operating system process identifier
Last call Minute	If the session STATUS is currently ACTIVE, then the value represents the elapsed time in seconds since the session has become active. If the session STATUS is currently INACTIVE, then the value represents the elapsed time in seconds since the session has become inactive.
Time of logon	Time of logon

See Also

Creating New Monitor - Oracle Database Server

MS SQL DB Servers

Supported Versions

Applications Manager supports monitoring of MS SQL 2000, 2005 and 2008 versions.

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Note:

Minimum User Privileges : User should be permitted to access MASTER database.

Roles : public + db_datareader should be selected in MASTER & msdb database

For MS SQL 2005 user role,

Database Accessed: Master

Permit in Database Role : db_datareader & Requires VIEW SERVER STATE permission on the server

To grant VIEW SERVER STATE you can use any of the following methods :

1) Execute the following query,

GRANT VIEW SERVER STATE TO username;

2) In SQL management studio for user choose Properties -> Securables -> Click Add (under securables) -> choose "All objects of the Types..." -> choose Servers -> choose Grant for "View server state" permission.

Monitor Information

Parameters	Description
Name	Specifies the name of MS SQL server monitor.
Health	Specifies the health (Clear, Warning, Critical) of the MS SQL server.
Type	Specifies the type you are monitoring.
Version	Specifies the version of the database server.
Port	Specifies the port number at which the database server is running.
ODBC Driver Version	Specifies the ODBC driver version used.
Host Name	Specifies the host at which the database server is running.
Host OS	Specifies the OS of the host where the database server is running.

Parameters	Description
Last Alarm	Specifies the last alarm that was generated for the database server.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.

Memory Usage

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

Buffer Manager Statistics

Parameters	Description
Buffer Hit Ratio	Percentage of pages that were found in the buffer pool without having to incur a read from disk.
Page LookUps/Min	Number of requests to find a page in the buffer pool.
Page Reads/Min	Number of physical database page reads issued.

Parameters	Description
Page Writes/Min	Number of physical database page writes issued.
Total Pages	Number of pages in the buffer pool (includes database, free, and stolen).
Database Pages	Number of pages in the buffer pool with database content.
Free Pages	Total number of pages on all free lists.

Connection Statistics

Parameters	Description
Connection Time	Time taken to get connected to the MS SQL database server.
Active Connections	Number of users connected to the system.
Logins/Min	Total number of logins started per minute.
Logouts/Min	Total number of logouts started per minute.

Cache Details

Parameters	Description
Cache Hit Ratio	Ratio between cache hits and lookups
Cache Used/Min	Times each type of cache object has been used
Cache Count	Number of cache objects in the cache
Cache Pages	Number of 8k pages used by cache objects

Lock Details

Parameters	Description
Lock Requests/Min	Number of new locks and lock conversions requested from the lock manager.
Lock Waits/Min	Total wait time for locks in the last minute.
Lock Timeouts/Min	Number of lock requests that timed out. This includes internal requests for NOWAIT locks.

Deadlocks/Min	Number of lock requests that resulted in a deadlock.
Average Lock Wait Time	The average amount of wait time for each lock request that resulted in a wait.

SQL Statistics

Parameters	Description
Batch Requests/Min	Number of SQL batch requests received by server.
SQL Compilations/Min	Number of SQL compilations.
SQL Recompilations/Min	Number of SQL re-compiles.
AutoParams/Min	Number of auto-parameterization attempts.
Failed AutoParams/Min	Number of failed auto-parameterizations.

Latch Details

Parameters	Description
Latch Waits/Min	Number of latch requests that could not be granted immediately and had to wait before being granted.
Average Latch Wait Time	Average latch wait time for latch requests that had to wait.

Access Method Details

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

Database Details

Parameters	Description
DataFile Details	Gives the DataFile size.
Log File Size	Gives the Size of the Log File, used size of the Log File.
Transaction Details	Gives the number of transaction per minute, replication transaction per minute, and the active transactions.
Log Flush Details	Gives the number of Log Flush/minute, Log Flush waits/minute, and the Log Flush wait time.

Scheduled Jobs

Parameters	Description
Job Status	Gives the Status of the job
Run date & time	Gives the date & time for which the jobs are scheduled to run.
Job Time	Gives the time taken by the job.
Retries Attempted	Gives the number of times the scheduled jobs attempted to run.

See Also

Creating New Monitor - MS SQL Database Server

IBM DB2 DB Servers

Supported Versions

Applications Manager supports monitoring of IBM DB2 8.x, 9 versions.

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Monitor Information

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

Connection Statistics

Parameters	Description
Connection Time	Time taken to get connected to the IBM DB2 database server
Total Connections	The total number of local and remote connections that currently present in the database manager
Local Connections	The number of connections initiated from remote clients to the current instance of the database manager
Remote Connections	The number of local applications that are currently connected to the database within the database manager

Agents Statistics

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

Database Information

Parameters	Description
Database Name	The real name of the database for which information is collected
Health	Specifies the health (Clear, Warning, Critical) of the database.
Database Alias	The alias of the database provided when calling the snapshot function
Database Path	The full path of the location where the database is stored on the monitored system

Database Status	The current status of the database
Connected Time	The date and time when the activate database was issued
Deadlock Rate	The total number of deadlocks that have occurred in the given polling interval
Percentage of Log Utilization	The total amount of active log space used in bytes in the database
Percentage of Sorts Overflowed	The percentage of sorts that have over flowed

Transaction Statistics

Parameters	Description
Successful Queries	The total number of successful SQL statements executed at the database in the given polling interval
Failed Queries	The number of SQL statements that were attempted, but failed at the database in the given polling interval
Units of Work	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

Cache Performance

Parameters	Description
Package Cache Hit Ratio	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.
Catalog Cache Hit Ratio	The hit ratio is a percentage indicating how well the catalog cache is helping to avoid actual accesses to the catalog on disk

Buffer Statistics

Parameters	Description
Buffer Pool Hit Ratio	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
Index Page Hit Ratio	The Index Page hit ratio indicates the percentage of time that the database manager accessed the index pages present in the buffer pools.
Data Page Hit Ratio	The Data Page hit ratio indicates the percentage of time that the database manager accessed the data pages present in the buffer pools.
Direct Reads	The number of read operations that do not use the buffer pool
Direct Writes	The number of write operations that do not use the buffer pool

TableSpace Status

Parameters	Description
Name	Refers to the name of the Table space.
Allocated Bytes	calculated from (tablespace_total_pages)*(tablespace_page_size) and converted to MB
Free Bytes	calculated from (tablespace_free_pages)*(tablespace_page_size) and converted to MB
% of Free Bytes	calculated from (tablespace_free_pages) /(tablespace_total_pages)*100

See Also

Creating New Monitor - IBM DB2 Database Server

Sybase DB Servers

Supported Versions

Applications Manager supports monitoring of Sybase ASE 12.5.3 and above.

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Monitor Information

Parameters	Description
Name	Specifies the name of Sybase server monitor.
Health	Specifies the health (Clear, Warning, Critical) of the Sybase server.
Type	Specifies the type you are monitoring.
Version	Specifies the version of the database server.
Port	Specifies the port number at which the database server is running.
Server Status	The current status of the database server itself
Started Time	The date and time that the database manager was started
Host Name	Specifies the host at which the database server is running.
Host OS	Specifies the OS of the host where the database server is running.
Last Alarm	Specifies the last alarm that was generated for the database server.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.

Memory Usage

Parameters	Description
Total Memory	Total memory used by ASE server in kb
Used Memory	Used memory available in ASE
Free Memory	Free memory available in ASE
Used Memory %	Percentage of memory used by ASE server

Connection Statistics

Parameters	Description
Connection Time	Time taken to get connected to the Sybase database ASE server
Active Remote Connections	The number of active remote connections after the ASE server has restarted
Max Remote Connections	The number of max remote connections available in the ASE server
Active User Connections	The number of active user connections after the ASE server has restarted
Max User Connections	The number of max user connections available in the ASE server

Database Details

Parameters	Description
Database Name	Name of the database instances
Total Size	Allocated space for the database in MB
Used Size	Used space of database in MB
Used Size %	Percentage of Used Size
Creator	User who created the database
Health	Health of the database

Current Process

Parameters	Description
Process Name	The name of the process currently connected to ASE server
Host/IPAddress	The Host Name / IP address of the process connected to ASE
User Name	The name in which the process is connected to ASE
DB Name	The name of the Database to which process is connected to ASE
Command	The command executed by process connected to ASE (command shown here limits to 255 chrs)
Status	The current status of the process
Physical_IO	The Physical_IO of the process
MemUsage	The memory used by the process
Time_Blocked secs	The time blocked by the process is shown in secs

Current Transactions

Parameters	Description
Type	The type of the transaction
Coordinator	The coordinator of the transaction
State	The state of the current transaction like it is started or in process or ended
Connection	The type of connection
DB Name	The database name in which the transaction is executed
Process Name	The process which is executing the transaction
Transaction Name	The name of the transaction
Starttime	The time at which the transaction started

See Also

Creating New Monitor - Sybase Database Server

PostgreSQL DB Servers

Supported Versions: 8.1 and above

The *Availability* tab displays the availability history of the PostgreSQL database servers in your network for the past 24 hours or 30 days. The *Performance* tab displays the Health Status and events for the past 24 hours or 30 days. The *List view* displays all the PostgreSQL servers that you monitor along with their current availability and health status. You can also perform bulk admin configurations from this view. Click on the individual monitors listed to view the following information:

Monitor Information

Parameter	Description
Name	Denotes the name of PostgreSQL database server monitor.
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the PostgreSQL server.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.

Connection Statistics

Parameter	Description
Active Connections	Number of currently active connections to the database
Total Users	The total number of users active at the time of data collection

Lock Statistics

Parameter	Description
Locks Held	Number of locks held by the indicated session
Locks Wait	Number of locks waiting in the database

Buffer Statistics

Parameter	Description
Buffer Hits/min	Total buffer hits (i.e., block read requests avoided by finding the block already in buffer cache) per minute
Block Reads/Min	Total disk blocks read per minute
Cache Hit Ratio	The current ratio of buffer cache hits to total requests

Disk Usage Details

Parameter	Description
Disk Usage	Size of the on-disk representation of all tables in the database in MB
Index usage	Size of the on-disk representation of all indexes in the database in MB

Index Scan Details

Parameter	Description
Index scans/min	Total number of index scans initiated per minute
Index Reads/min	Total number of index entries returned by index scans per minute
Index Fetches/min	Total number of live table rows fetched by simple index scans per minute

Query Statistics

Parameter	Description
Row inserts/min	Total numbers of rows returned by each type of scan per minute
Row Updates/min	Total of row insertions and updates per minute
Row Deletes/min	Total number of rows deleted per minute

Transaction Details

Parameter	Description
Total Commits	Total transactions committed
Total Rollbacks	Total transactions rolled back
Commits/Min	Total transactions committed per minute
Rollbacks/Min	Total transactions rolled back per minute

Table Level Scan Details

Parameter	Description
Sequential Scans/min	Total number of sequential scans per minute
Table Index Scans/min	Total number of index scans per minute
Sequential Scan Rows Read/min	Total number of rows returned by sequential scans per minute
Table Index Scan Rows Read/min	Total numbers of rows returned by index scans per minute

Primary Database Object Statistics

Parameter	Description
Total Tables	Total number of tables in the database server
Total Triggers	Total number of triggers in the database server

Parameter	Description
Total Procedures	Total number of procedures in the database server
Size of the Largest Table	Size of the largest table in the database server
Largest Table(s)	Largest table in the database server

See Also

[Creating New Monitor - PostgreSQL Database Server](#)

Memcached Servers

Supported Versions: Memcached v1.2 and above.

Monitored Parameters

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

The *Availability* tab shows the Availability history of the Memcached server for the past 24 hours or 30 days. The *Performance* tab shows the Health Status and events for the past 24 hours or 30 days. The *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed to view the following information:

Parameters	Description
Monitor Details	
Availability	Shows the current status of the Memcached server - available or not available
Performance Status	
Used Memory	Specifies the used memory of the server in percentage
Free Memory	Specifies the free memory of the server in percentage
Hit Ratio	Refers to the hit ratio in percentage
Memory Utilization	
Used Memory	Specifies the used memory of the server in mega bytes
Free Memory	Specifies the free memory of the server in mega bytes
Total Memory	Specifies the total memory of the server in mega bytes
CPU Utilization	
User CPU *	Specifies the accumulated user time for a process in seconds
System CPU *	Specifies the accumulated system time for a process in seconds
Cached Hits and Misses	
Hits/min	Number of keys that have been requested and found present per minute
Misses/min	Number of items that have been requested and not found per minute

Parameters	Description
GET and SET Requests	
Gets/min	Number of retrieval requests per minute
Sets/min	Number of storage requests per minute
Cached Items	
Items cached	Current number of items stored by server
Evictions	Number of valid items removed from cache to free memory for new items
Network Traffic	
Bytes Received	Number of bytes read by this server from network per min
Bytes Sent	Number of bytes sent by this server to network per min
Current Connections	
Connections	Number of open connections
Response Time	
Response Time	The time taken by Applications Manager to execute the STATS command on the memcached server
Version	Version of Memcached server
Transaction	
SET-Time	The time taken by Applications Manager to set the content on the memcached server
GET-Time	The time taken by Applications Manager to fetch the content from the memcached server
DELETE-Time	The time taken by Applications Manager to delete the content from the memcached server
Total Transaction Time	The total time taken to connect to memcached server, set content, fetch content and delete content from the server

* - not supported in Memcached installed in Windows

See Also

Creating New Monitor - Memcached Server

Middleware / Portal

Applications Manager provides Middleware / Portal monitoring that monitors system resources. It also provides proactive measures by notifying system operators about potential problems.

The different middleware / portal supported are:

- Microsoft Message Queue (MSMQ)
- Microsoft Office Sharepoint Server **Add On!**
- WebLogic Integration
- IBM WebSphere MQ **Add On!**
- VMware vFabric RabbitMQ

Browse through the different servers that provide server information and their parameters being monitored.

See Also

Creating New Monitor - Middleware / Portal

Microsoft MQ (MSMQ)

Monitored Parameters

Applications Manager monitors the critical components of Microsoft Message Queue (MSMQ) servers to detect any performance problems. These components include message stats, session stats, Microsoft message queue stats, etc.

The *Availability* tab shows the availability history of the MSMQ for the past 24 hours or 30 days. The *Performance* tab shows the response time of the MSMQ as well as the health status and events for the past 24 hours or 30 days.

The *List view* lists all the MSMQ servers monitored by Applications Manager along with their overall availability and health status. You can also perform bulk admin configurations from this view. Click on the individual monitors listed to view detailed performance metrics.

Parameter	Description
Monitor Information	
Name	The name of the Microsoft Message Queue Server (MSMQ) monitor.
Type	Describes the type of monitor.
Health	Represents the health (Clear, Warning, Critical) status of the MSMQ server.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the monitor for the day. You can also view 7/30 reports and the current availability status of the monitor.
Microsoft Message Queue Services	
Service Name	The name of the message queue service.
Status	The current status of the message queue service.
Messages Stats	
Incoming messages/sec	The rate at which incoming Message Queuing messages are placed in queues on the selected computer by the Message Queuing service.
Outgoing messages/sec	The rate at which outgoing Message Queuing messages are sent from the selected computer by the Message Queuing service.

Parameter	Description
MSMQ Incoming Messages	The total number of incoming Message Queuing messages placed in queues on the selected computer by the Message Queuing service.
MSMQ Outgoing Messages	The total number of outgoing Message Queuing messages sent from the selected computer by the Message Queuing service.
Total bytes in all Queues	The total number of bytes in all Message Queuing messages residing in active queues on the selected computer.
Total messages in all Queues	The total number of Message Queuing messages residing in active queues on the selected computer.
Session Stats	
Sessions	The total number of open network sessions involving the selected computer.
IP Sessions	The number of open IP sessions involving the selected computer.
Incoming Multicast Sessions	The number of open incoming multicast sessions involving the selected computer.
Outgoing Multicast Sessions	The number of open outgoing multicast sessions involving the selected computer.
Outgoing HTTP Sessions	The number of open outgoing HTTP sessions involving the selected computer.
Microsoft Message Queue Stats	
Queue Name	The name of the Message queue.
Bytes in Journal Queue	The total number of bytes in all Message Queuing messages that currently reside in the selected journal.
Bytes in Queue	The total number of bytes in all Message Queuing messages that currently reside in the selected queue.
Messages in Journal Queue	The total number of Message Queuing messages that currently reside in the selected journal.
Messages in Queue	The total number of Message Queuing messages that currently reside in the selected queue.

See Also

Creating New Monitor - Microsoft MQ (MSMQ)

Microsoft Office Sharepoint Servers

Monitored Parameters

Microsoft Office Sharepoint Servers are monitored based on the attributes such as Office Search Gatherer, etc. The monitoring details of Microsoft Office Sharepoint Servers 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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Name	Name of the monitor
Health	Health of the monitor
Last Polled at	Time at which last poll happened
Next Polled at	Time at which the next poll has been scheduled
Availability	Availability of the monitor
Office Search Gatherer	
Reason To Back Off	Info on why Gatherer service went into back off state
Active Queue Length	The number of documents waiting for robot threads.
Threads In Plugins	The number of threads waiting for plug-ins to complete an operation.
Delayed Documents	The number of documents delayed due to site hit frequency rules.
Idle Threads	The number of threads waiting for documents.
Documents Delayed Retry	The number of documents that will be retried after time-out.
Threads Accessing Network	The number of threads waiting for a response from the filter process.
Excel Services Web Frontend	
Active Requests	Number of active requests being processed at sampling time

Parameter	Description
Requests Per Second	Number of requests per second at sampling time
Excel Calculation Services	
Requests With Errors Per Sec	Number of requests that are returned with errors per second on Excel Calculation Services between sampling times
Sessions Per Second	Average number of sessions opened per second between the last two samples
Cached Charts Requested Per Sec	Number of charts that are provided from a cached image
Active Sessions	Number of active sessions on Excel Calculation Services at sampling time
Rendered Charts Requested Per Sec	Number of chart requests per second
Active Requests	Number of active requests being processed on Excel Calculation Services at sampling time
Requests Received Per Sec	Number of requests received per second on Excel Calculation Services between sampling times
Excel WebAccess	
Excel Web Access Request Time	Excel Web Access Average Request time between the last two samples
Chart Image Requests per Second	The number of requests for chart images served by Excel Web Access per second
Average Chart Image Request Time	The average time it takes between the request for a chart image and the issuance of the response to the web browser by Excel Web Access
Document Conversions	
Incoming EMail Messages Processed	The rate at which e-mail messages have been received and processed by SharePoint
Pending Conversions	The number of pending document conversions
Active Server Pages	
Errors/sec	The number of errors per second.

Parameter	Description
Requests Queued	The number of requests waiting for service from the queue.
Requests Rejected	The total number of requests not executed because there were insufficient resources to process them.
Requests/sec	The number of requests executed per second.
Current Sessions	The current number of sessions being serviced
Transactions/sec	Transactions started per second.
Pending Transactions	Number of transactions in progress
Memory Stats	
Free Memory in MB	Free Memory
Page Faults Per Sec	Average number of pages faulted per second.
% Committed Bytes In Use	ratio of Memory\\Committed Bytes to the Memory\\Commit Limit.
% Processor Time	percentage of elapsed time that the processor spends to execute a non-idle thread.
Office Search Archival Plugin	
Active Docs in First Queue	The number of documents actively using the first queue.
Total Docs in First Queue	The total number of documents which have used the first queue.
Active Docs in Second Queue	The number of documents actively using the second queue.
Total Docs in Second Queue	The total number of documents which have used the second queue.
Total Documents	The number of documents processed.
Error Documents	The number of documents which returned errors from the plug-in.
Active Queue	The currently active queue.
Bulk Insert Sessions	The number of active bulk insert sessions to the database server.

Parameter	Description
Office Search Schema Plugin	
Aliases Loaded	The total number of aliases currently loaded.
Aliases Mapped	The total number of aliases which have been mapped.
Duplicate Aliases	The number of aliases ignored since they are duplicates.
Error Documents	The number of documents which returned errors from the plug-in.
Refresh Count	The number of aliases refreshes done from the database.
Total Documents	The number of documents processed.
Total Properties Processed	The number of properties processed by the plugin.
Office Server Search Indexer Catalogs	
Failed Queries	Number of queries failed
Succeeded Queries	Number of queries succeeded
Queries	Number of queries
Documents Filtered	Number of documents filtered
Index Size	Size of index
Share Point Server Services	
Service Name	Name of the Windows Service
Status	Status of the service whether it is Running or Stopped
Health	Health of the Service depending upon the Availability of Service
Availability	Availability is down when the service is in stopped state and up when in Running state
Web Content Management-Publishing Cache	
Publishing Cache Hit Ratio	The ratio of hits to misses on the Publishing cache.
Total Object Discards	The total number of items that have been removed from the Publishing cache due to cache compaction.

Parameter	Description
Publishing Cache Hits / sec	The hit rate on the Publishing cache.
Publishing Cache Misses / sec	The miss rate on the Publishing cache.
Publishing Cache Flushes / sec	The rate that we are updating the cache due to site changes.

See Also

Creating New Monitor - Microsoft Office Sharepoint Server

WebLogic Integration Servers

Supported Version

WebLogic Integration Server 8.x

Monitored Parameters

WebLogic Integration servers are monitored based on a parameters/ attributes like Business Process Details, Application Integration details & Message Broker details. These attributes provide information about the functioning of WebLogic Integration server monitor and you can receive alarms based on the thresholds configured on the attributes of the server.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information. The WebLogic Server parameters are shown along with the Weblogic Integration Server parameters in the monitor details page.

Parameters	Description
Business Process Details	
Process Name	Name of the Process.
Health	Health of the process, depends on the below given parameters.
Avg Elapsed Time	Specifies the average elapsed time of the process. Elapsed time is the time elapsed since all the instances started.
Completed Instances	Specifies the number of instances completed per minute
SLA Exceeded Instances	Shows the number of instances where SLA exceeded
Running Instances	Shows the number of instances running currently
Aborted Instances	Shows the number of instances that were aborted - threw an unhandled exception
Frozen Instances	Shows the number of instances running frozen - failed but can be unfrozen. When an instance is unfrozen, it resumes from the point where it failed.
Terminated Instances	Shows the number of instances that were terminated

Parameters	Description
Application Integration Details	
AppView Name	Application View ID
Health	Health of the Application
Service Count	Number of service invocations since the service counter was last reset
Service Error Count	Number of service errors since the service counter was last reset plus the number of event delivery errors since the event counter was last reset.
Avg. Service Elapsed Time	Average elapsed time in milliseconds for service invocations. This number averages elapsed time for both synchronous and asynchronous services. For asynchronous services, elapsed time includes only time spent communicating with the adapter and excludes time spent waiting on the asynchronous request queue..
Event Count	Number of events delivered since the event counter was last reset..
Event Error Count	Number of event delivery errors since the event counter was last reset.
Message Broker Details	
Channel Name	Specifies the name of the Channel
Health	Specifies the health of the Channel, depends on the Message Count, Subscriber Count & Dead Letter Count
Message Count	Specifies the number of messages delivered to this channel.
Subscriber Count	Specifies the number of process or Web service types that can subscribe to the channel.
Dead Letter Count	When the Message Broker is unable to determine the URI to send a message to (that is, no subscribers are found), the message is sent to the appropriate deadletter channel: /deadletter/xml, /deadletter/string, or /deadletter/rawData. The Dead Letter Count specifies the number of messages sent to the dead letter channels since the count was last reset.

See Also

Creating New Monitor - WebLogic Integration Server

IBM WebSphere MQ

Monitored Parameters

IBM WebSphere MQ servers are monitored based on the attributes such as listener stats, channel monitoring, etc. and the different web applications and EJB deployed in the server. The monitoring details of IBM WebSphere MQ 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.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Name	The Display name of the Monitor
Health	Represents the health status
Last Polled at	Time at which the previous poll had started
Next Poll at	Time at which the next poll has been scheduled
Availability	Shows the current status of the server - available or not available.
Channel Monitoring	
Channel Name	Name of the Channel
Status	Status of the channel - running
Bytes Sent	Number of bytes sent
Bytes Received	Number of bytes Received
Buffers Sent	Number of buffers sent
Buffers Received	Number of buffers Received
Availability	Availability of Channel,based on the status attribute.If the status of the channle is RUNNING then it is considered to be available .If the channel is in other states then it is considered to be down.

Parameter	Description
Health	Health of the Channel based on all the above attributes
listener Stats	
Listener Name	Specifies the name of the Listener
Status	The current status of the listener. The value can be:Initializing,Running, Stopping
Session Count	The number of sessions that the listener can use. This is valid only on Windows.
Backlog	The number of concurrent connection requests that the listener supports.
Health	Health of the Listener based on all the above attributes
Queue Monitoring	
Queue Name	Name of the Queue
Current Depth	Current queue depth.
% of Queue Occupied	Percentage of Queue Depth occupied against the max Queue Depth.
Open Input Count	Open input count (parameter identifier: MQIA_OPEN_INPUT_COUNT).
Open Output Count	Open output count (parameter identifier: MQIA_OPEN_OUTPUT_COUNT)
Health	Health of the Queue based on all the above attributes

You can also compare the values between the various attributes.

See Also

Creating New Monitor - IBM WebSphere MQ

VMware vFabric RabbitMQ

Applications Manager monitors the critical components of VMware vFabric RabbitMQ servers to detect individual queues and collect metrics which reflect the queue's performance and throughput.

The critical components of RabbitMQ servers include:

- Queued messages and message rates statistics
- Node details like socket descriptor and Erlang process utilization
- Channel statistics like message publish rates
- Exchange message rates
- In depth connection status

Monitored Parameters:

RabbitMQ monitoring includes delivering proactive alarm notifications during network congestion, checking if a consumer is processing slowly or has gone down under heavy message traffic, identifying performance bottlenecks due to high socket descriptors utilization and generating historical reports.

The *Availability* view shows an availability history bar graph of the RabbitMQ server. Using the drop-down list at the right-hand corner of the page, you can set the bar chart to show availability history for the past 24 hours or 30 days.

The *Performance* tab gives a graphical representation of the publish, delivery, acknowledged and unacknowledged rates of RabbitMQ server as well as the health history for the past 24 hours or 30 days. The colored icons at the corners of the graphs pop up a 'heat chart' for the respective metric rate.

The *List view* lists all the RabbitMQ servers monitored by Applications Manager along with their overall availability and health status. You can edit the monitor details and configure alarms from the list. You can also perform bulk admin configurations from this view. Click on the individual monitors listed to view detailed performance metrics.

The table below gives a detailed description of the parameters displayed in each of the tabs:

OVERVIEW	
Parameter	Description
Monitor Information	General details like name, type, health, host name, etc.

OVERVIEW	
Availability history for last 6 hours	Bar graph showing the availability history of the server for the last six hours.
Performance history for last 6 hours	Chart showing the performance history of the server for the last six hours.
Queued Messages	Message vs time graph showing the ready and unacknowledged messages.
Message Rates	Message per second vs time graph showing the deliver, acknowledged and publish rates
Socket descriptors used/available/utilization	The number of concurrently open/available/used socket descriptors for the monitor.
Erlang processes used/available/utilization	The number of concurrently open/available/used Erlang processes for the monitor.
QUEUES	
Parameter	Description
Name	The name of the message queue.
Exclusive	Number of messages of the exclusive consumer subscribed to this queue.
Messages Ready	Number of messages ready to be delivered to clients.
Messages Unacknowledged	Number of messages delivered to clients, but not unacknowledged yet (meaning it is in progress or has been reserved).
Total Messages	Sum of ready and unacknowledged messages (queue depth)
Incoming rate	The rate at which messages are received.
Deliver/Get rate	The rate at which messages are delivered.
Ack rate	The rate at which messages are acknowledged.
EXCHANGES	
Parameter	Description
Name	The RabbitMQ exchange name.
Type	The exchange type (one of direct, topic, headers, fanout).
Incoming Publish rate	The per second rating of incoming messages.

Outgoing Publish rate	The per second rating of outgoing messages.
CHANNELS	
Parameter	Description
Channel	The channel through which messages are sent.
User Name	The RabbitMQ username associated with the channel.
Prefetch msgs	QoS prefetch count value for the channel.
Unacked msgs	Number of messages delivered via this channel, but not yet acknowledged.
Unconfirmed msgs	Number of published messages not yet confirmed. On channels not in confirm mode, this remains 0
Publish rate msgs/sec	The per second publishing rate of messages.
DeliverGet rate msgs/sec	The per second receiving rate of messages.
Ack rate msgs/sec	The per second acknowledgment rate of messages.
CONNECTIONS	
Parameter	Description
Peer Address	The IP address of the host on the other side of the connection.
Protocol	Version of the AMQP protocol in use (currently one of {0,9,1} or {0,8,0})
Receive rate kbps	Rate at which the message is being received.
Send rate kbps	Rate at which the message is being sent.
State	Connection state (one of [starting, tuning, opening, running, closing, closed])

You can enable, disable or delete any of the nodes, queues, exchanges, channels or connections from the drop-down menu at the bottom of the page. You can also compare reports from an adjacent drop-down list.

See Also

Creating New Monitor - RabbitMQ

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 (Page Space Details)
5. IBM AS400/iSeries
6. HP Unix
7. Tru64 Unix
8. FreeBSD
9. Mac OS
10. Novell

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameters	Description
System Load	Specifies the number of jobs handled by the system in 1/ 5/ 15 minutes with its peak and current value, and current status.
Disk Utilization	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.)

Parameters	Description
Memory Utilization	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.
Disk I/O Stats	specifies read/writes per second, transfers per second, for each device.
CPU Utilization	Specifies the total CPU used by the system with its peak and current value, and current status.

Note: Option is provided for **ignoring the monitoring of specific disk** drive in a server. Open <AMServer.properties> file in <AppManager Home/Conf> and add the drive that you dont want to monitor to <am.disks.ignore>. For eg.,

The drives begining with the characters given below will not be monitored in server monitor.
am.disks.ignore=C:

Here, monitoring will not happen for C: drive. Likewise, you can add further disks comma separated(C;D;./home).

The following table briefs the parameters monitored & the mode of monitoring (✓- yes).

Note: If the server monitor is added in Telnet & SSH mode, you have the option to **directly access Telnet client** by clicking on the 'Execute Commands on this server' link found below Today's Availability pie chart. This option is disabled by default.

To enable it, permissions need to be given to admin or operator to use this telnet client. The permissions can be given from *Admin tab->User Administration --> Permissions* link.

Operating System	Telnet	SSH	SNMP	WMI
Windows			✓	✓ (only if Applications Manager is installed on windows machine)
Linux	✓	✓	✓	
Solaris	✓	✓	✓	
HP-UX / Tru64 Unix	✓	✓		

Operating System	Telnet	SSH	SNMP	WMI
FreeBSD	✓	✓	✓	
Mac OS	✓	✓	✓	
IBM AIX	✓	✓		
Novell			✓	
Attributes				
CPU Utilization (all types except Windows NT)	✓	✓	✓	✓
Disk Utilization (all types)	✓	✓	✓	✓
Physical Memory Utilization (IBM AIX -only for root user, Windows - WMI mode, all other types)	✓	✓	✓	✓
Swap Memory Utilization (IBM AIX - only for root user, FreeBSD, Linux, Solaris, Windows, Novell)	✓	✓		✓
Network Interface (all types)			✓	✓ [status attribute data is not available]
Process Monitoring (all types)	✓	✓	✓	✓
Process Monitoring - Memory Utilization (all types)	✓	✓	✓	✓
Process Monitoring - CPU Utilization (IBM AIX - FreeBSD, Linux, Mac OS, Solaris, HP Unix / Tru64)	✓	✓	✓	
Service Monitoring (only for Windows)				✓
Event log (only for Windows)				✓
System Load (IBM AIX, FreeBSD, Linux, Mac OS, HP-Unix, Solaris, Novell)	✓	✓	✓	

Operating System	Telnet	SSH	SNMP	WMI
Disk I/O Stats (only for IBM AIX, Linux, Solaris, Novell)	✓	✓		

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

When it comes to choosing the mode of monitoring for servers, we recommend Telnet/SSH over SNMP.

Page Space in AIX Servers:

To get in-depth details on **Page Space** in AIX servers, you can use the following command "**lsps -a**".

The command "**lsps -a**" lists the location of the paging space logical volumes as they were, not as they are.

Normally page spaces are used when the process running in the system has used the entire allocated memory and it has run out of memory space. It then uses the page spaces in the system to move the piece of code/data that is not currently referenced by the running process into the page space area so that it could be moved back to the Primary memory when it is been referenced again by the currently running process.

While trying to monitor the AIX server, if you get "**No data Available**" for Page Space, you can troubleshoot it by following the steps given below:

First, you need to establish connection only through **TELNET** or **SSH** mode.

Second, check whether the command **lsps -a** exists in the system and then execute it.

Displaying Paging Space Characteristics

The "**lsps**" command displays the characteristics of paging spaces, such as the paging space name, physical volume name, volume group name, size, percentage of the paging space used, whether the space is active or inactive, and whether the paging space is set to automatic. The paging space parameter specifies the paging space whose characteristics are to be shown.

The following examples show the use of **lsps** command with various flags to obtain the paging space information. The "**-c**" flag will display the information in colon format and paging space size in physical partitions.

lsps -a

Page Space	Physical Volume	Volume Group	Size	%Used	Active	Auto	Type
paging00	hdisk1	rootvg	80MB	1	yes	yes	lv
hd6	hdisk1	rootvg	256MB	1	yes	yes	lv

Adding and Activating a Paging Space

To make a paging space available to the operating system, you must add the paging space and then make it available. The total space available to the system for paging is the sum of the sizes of all active paging-space logical volumes.

Note: You should not add paging space to volume groups on portable disks because removing a disk with an active paging space will cause the system to crash.

You can get more details about the command here: <http://web.utahnet.at/mario/exam/5129c72.htm>

Apart from the above mentioned parameters, you can also monitor the following

Processes**Windows Services****Network Interface****To monitor processes in a server**

1. In the Server Monitor page 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 alarms 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.

To monitor windows services

Note: Windows Services monitoring is possible only in **WMI mode** of monitoring

1. In the Windows Monitor page, under **Service Details**, click **Add New Service**
2. All the services that are running would be displayed along with service name and status.
3. Select the services that you want to monitor.

After configuring the services, they are listed under the **Service Details** section of the Windows Monitor page. By clicking on the service, you can view its availability graph. You can also configure alarms for the availability of that particular service.

Apart from monitoring the availability of the service, you can manage the services by using the *start*, *stop*, *restart* options. When the service goes down, you can configure action "Restart the Service " along with other actions.

To monitor Network Interfaces

Note: Network Interface monitoring is possible only in **SNMP** and **WMI mode** of monitoring

In the Server Monitor page, under **Network Interfaces**, all the network interfaces will be listed. The various attributes that can be monitored are:

- Interface Traffic - Input traffic (bits received), Output Traffic (bits transmitted). You can set alarm thresholds for these attributes.
- Interface utilization - Input Utilization %, Output Utilization %. You can set alarm thresholds for these attributes.
- Packets received - Packets received per second
- Packets transmitted - Packets transmitted per second
- Error packets - No.of packets in error per second after receiving the packets
- Discarded packets - No.of packets discarded per second after receiving the packets
- Health - the health of the interface based on the attributes
- Status - whether the interface is up or down (shown only in SNMP mode of monitoring)

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

Windows Servers

This section deals with the performance metrics displayed for windows servers. Refer this page for information about other servers supported by Applications Manager.

Monitored Parameters

Applications Manager monitors the critical components of Windows servers to detect any performance problems. These components include CPU, memory, disk, network traffic, etc.

The *Availability* tab shows the availability history of the Windows server for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the Windows server such as physical memory utilization, CPU utilization, response time and swap memory utilization along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* lists all the Windows servers monitored by Applications Manager along with their overall availability and health status. It enables you to perform bulk admin configurations. Click on the individual monitors listed to view detailed performance metrics. The list view also shows the **virtual machines (Windows guest OS)** configured in your data center along with their availability and health status.

To view detailed performance metrics of a Windows server, click on the monitor name listed in the *Availability* or *List View* tabs. The performance metrics have been categorized into 6 different tabs:

- Overview
- CPU
- Disk
- Network
- Event Log
- Configuration

Overview

This tab provides a high-level overview of the health and performance of the Windows server along with information pertaining to the processes and services running on the system.

Parameters	Description
Monitor Information	
Name	The name of the Windows server monitor
System Health	Denotes the health status of the Windows server (clear, critical, warning)
Type	Denotes the type you are monitoring
Host Name	The host name of the Windows system
Host OS	The main OS installed on the system
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the server for the day. You can also view 7/30 reports and the current availability status of the server.

You can use the Custom Fields option in the 'Monitor Information' section to configure additional fields for the monitor.

The overview tab shows dials for CPU, memory and disk utilization. You can click on these dials to view detailed graphs and charts for these attributes. The graphs available are History report, hour of day report, day of week report and heat chart. These graphs can be generated for both real time and historical data.

The **CPU and memory utilization - last six hours** graph shows the memory usage and CPU usage values for the last six hours. The attributes shown here are swap memory utilization, physical memory utilization (in % and MB), free physical memory (MB) and CPU utilization (%).

The **Breakup of CPU Utilization** graph provides a break up of metrics for the entire system processor with attributes such as run queue, user time(%), system time(%), I/O wait(%), idle time(%) and interrupts/sec.

The **Process Details** section shows information about the processes running in the Windows server. You can add processes for monitoring using the *Add New Process* option. You can also delete unwanted processes and enable/disable reports for specific processes. Click on any of the attributes listed to view more details.

The **Service Details** section shows the availability of services running in the Windows server. You can add services for monitoring using the *Add New Service* option. You can also stop, start, restart and delete services from within Applications Manager itself.

The **Monitors in this System** section shows the availability and health of the monitors configured in this server. To add new monitors for monitoring, use the *Add Monitors* option.

CPU

This tab provides the CPU usage statistics of the Windows server. The tab includes two graphs - one that displays the *CPU utilization by CPU Cores* and another that shows the *Breakup of CPU utilization - by CPU cores*. You can view additional reports by clicking the graphs present in the *Breakup of CPU Utilization - by CPU cores* section. These reports include Break up of CPU Utilization (%) Vs Time, User Time (%) Vs Time, System Time (%) Vs Time, I/O Wait Time (%) Vs Time, Idle Time (%) Vs Time, CPU Utilization (%) Vs Time and Interrupts/sec Vs Time for all the CPU cores.

The CPU tab also shows the following performance metrics:

Parameter	Description	Monitoring Mode	
Core	The name of the CPU core		
User Time(%)	The percentage of time that the processor spends on User mode operations. This generally means application code.	✗	
System Time(%)	The percentage of CPU kernel processes that are in use.	✗	
I/O Wait Time(%)	The time spent by the processor to waiting for I/O to complete.	✗	
Idle Time(%)	The time when the CPU is idle (not being used by any program)	✓	
CPU Utilization(%)	Specifies the total CPU used by the system	✗	
Interrupts/sec	The rate at which CPU handles interrupts from applications or hardware each second. If the value for Interrupts/sec is high over a sustained period of time, there could be hardware issues.	✗	

You can also view graphs for these attributes by selecting the necessary CPU core and then choosing the appropriate attribute.

Disk

This tab displays disk usage and disk I/O statistics of the Windows server.

Parameters	Description
Disk Utilization	
Disk	The name of the disk drive
Used(%)	Denotes how much disk space out of the total disk space has actually been used (in percentage)
Used(MB)	The disk space used in mega bytes
Free(%)	The percentage of total usable space on the disk that was free.
Free(MB)	The unallocated space on the disk in mega bytes.

Disk I/O Statistics:

Parameter	Description	Monitoring Mode	
Transfers/sec	The number of read/write operations on the disk that occur each second.	✗	
Writes/sec	The percentage of elapsed time that the disk drive was busy servicing write requests.	✗	
Reads/sec	The percentage of elapsed time that the disk drive was busy servicing read requests.	✗	
% Busy Time	The percentage of time the disk was busy.	✗	
Average Queue Length	The average number of both read and write requests that were queued for the disk during the sample interval.	✗	

You can also delete disks that have been physically removed using the **Delete Orphaned Disk** option.

Network

This tab contains metrics related to network interfaces.

Parameters	Description
Network Interface	
Name	The name of the network interface present in the Windows system.
Speed(Mbps)	The estimate of the current bandwidth in Mbps
Input Traffic(Kbps)	The rate at which packets are received on the interface, in kilo bytes per second.
Output Traffic(Kbps)	The rate at which packets are sent on the interface, in kilo bytes per second.
Errors	Number of packets that could not be sent or received.

You can also delete interfaces that have been physically removed using the **Delete Orphaned Interface** option.

Event Log

This tab shows information pertaining to the recent Windows events.

Parameters	Description
Rule Name	The name of the event log rule.
Log File Type	The type of the Windows event log file.
Source	The source that generated the event.
Event Id	The identifier of the event.
Type	The type of the event.
User Name	User name of the logged-on user when the event occurred. If the user name cannot be determined, this will be None.
Description	Description of the event.
Generated Time	The time when the event was generated.

Configuration

This tab contains information about system configuration attributes.

Parameters	Description
System Information	
Host Name	The name of the system.
Manufacturer	The name of the machine manufacturer.
Model	Product name that a manufacturer gives to the computer.
Domain	The name of the domain to which the system belongs.
BIOS Version	The current BIOS version that is running on the motherboard of the system
OS Information	
OS Name	The name of the operating system instance.
OS Version	Version number of the operating system.
OS Release	The latest service pack installed on the computer. If no service pack is installed, the value will be '-'
Manufacturer	Name of the operating system manufacturer. For Windows-based systems, this value is "Microsoft Corporation".
OS Installed Date	The date the OS was installed on the system.
Registered User	Name of the registered user of the operating system.
Windows Directory	Windows directory of the operating system.
OS Language	Language version of the operating system installed.
Memory Information	
Total Physical Memory (MB)	Total amount of physical memory as available to the operating system.
Total Virtual Memory (MB)	The total amount of area on the hard disk that windows uses as if it were RAM.

Processor Information	
Id	Unique identifier of a processor on the system
Model	The processor model type
Implementation	The processor family type.
Manufacturer	Name of the processor manufacturer
Speed(MHz)	Current speed of the processor
Cache (KB)	Size of the processor cache. A cache is an external memory area that has a faster access time than the main memory.
Network Interface Settings	
Name	The name of the network adapter.
IP Address	The IP address configured for this network interface
Type	The network medium in use.
Mac Address	The Media access control address for this network adapter. A MAC address is a unique 48-bit number assigned to the network adapter by the manufacturer. It uniquely identifies this network adapter and is used for mapping TCP/IP network communications.
Manufacturer	The name of the network adapter's manufacturer
Status	The current status of the network adapter
Printer Settings	
Name	Name of the printer
Server	Name of the server that controls the printer. If this value is not shown, it means the printer is controlled locally.
Type	Denotes whether the printer is controlled locally or remotely
Default	Indicates whether the printer is the default one. Values are either True or False.
Status	Current status of the printer
Location	Physical location of the printer

See Also

Creating New Windows Server Monitor

Linux Servers

Monitored Parameters

Applications Manager monitors the key performance indicators of Linux servers to detect any performance problems. These indicators include CPU, memory, disk, etc.

The *Availability* tab shows the availability history of the Linux server for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the Linux server such as physical memory utilization, CPU utilization, response time and swap memory utilization along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* lists all the Linux servers monitored by Applications Manager along with their overall availability and health status. It enables you to perform bulk admin configurations. Click on the individual monitors listed to view detailed performance metrics.

To view detailed performance metrics of a Linux server, click on the monitor name listed in the *Availability* or *List View* tabs. The performance metrics have been categorized into 4 different tabs:

- Overview
- CPU
- Disk
- Configuration

Overview

This tab provides a high-level overview of the health and performance of the Linux server along with information pertaining to the processes and services running on the system.

Parameters	Description
Monitor Information	
Name	The name of the Linux server monitor.
System Health	Denotes the health status of the Linux server (clear, critical, warning).
Type	Denotes the type you are monitoring.
Host Name	The host name of the Linux system.
Host OS	The main OS installed on the system.
Last Polled at	Specifies the time at which the last poll was performed.

Parameters	Description
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the server for the day. You can also view 7/30 reports and the current availability status of the server.

You can use the Custom Fields option in the 'Monitor Information' section to configure additional fields for the monitor.

The overview tab shows dials for CPU, memory and disk utilization. You can click on these dials to view detailed graphs and charts for these attributes. The graphs available are History report, hour of day report, day of week report and heat chart. These graphs can be generated for both real time and historical data.

The **CPU and memory utilization - last six hours** graph shows the memory usage and CPU usage values for the last six hours. The attributes shown here are swap memory utilization, physical memory utilization (in % and MB) and CPU utilization (%).

The **Breakup of CPU Utilization** graph provides a break up of performance metrics for the entire system processor with attributes such as run queue, blocked process, user time(%), system time(%), I/O wait(%), idle time(%) and interrupts/sec.

The **System Load** graph provides you an idea of the amount of work that the system performs. The system load during the last one-, five- and fifteen-minute periods are represented by parameters such as Jobs in Minute, Jobs in 5 minutes and Jobs in 15 minutes.

The **Process Details** section shows information about the processes running on the Linux server. You can add processes for monitoring using the *Add New Process* option. You can also delete unwanted processes and enable/disable reports for specific processes. Click on any of the attributes listed to view more details.

The **Monitors in this System** section shows the availability and health of the monitors configured in this server. To add new monitors for monitoring, use the *Add Monitors* option.

CPU

This tab provides the CPU usage statistics of the Linux server. The tab includes two graphs - one that displays the *CPU utilization by CPU Cores* and another that shows the *Breakup of CPU utilization - by CPU cores*. You can view additional reports by clicking the graphs present in the *Breakup of CPU Utilization - by CPU cores* section. These reports include Break up of CPU Utilization (%) Vs Time, User Time (%) Vs Time, System Time (%) Vs Time, I/O Wait Time (%) Vs Time, Idle Time (%) Vs Time, CPU Utilization (%) Vs Time and Interrupts/sec Vs Time for all the CPU cores.

The CPU tab also shows the following performance metrics:

Parameter	Description	Monitoring Mode	
Core	The name of the CPU core		
User Time(%)	The percentage of time that the processor spends on User mode operations. This generally means application code.	✓	
System Time(%)	The percentage of CPU kernel processes that are in use.	✓	
I/O Wait Time(%)	The time spent by the processor to waiting for I/O to complete.	✓	
Idle Time(%)	The time when the CPU is idle (not being used by any program)	✓	
CPU Utilization(%)	Specifies the total CPU used by the system	✓	
Interrupts/sec	The rate at which CPU handles interrupts from applications or hardware each second. If the value for Interrupts/sec is high over a sustained period of time, there could be hardware issues.	✓	

You can also view graphs for these attributes by selecting the necessary CPU core and then choosing the appropriate attribute.

Disk

This tab displays disk usage and disk I/O statistics of the Linux server.

Parameters	Description
Disk Utilization	
Disk	The name of the disk drive
Used(%)	Denotes how much disk space out of the total disk space has actually been used (in percentage)
Used(MB)	The disk space used in mega bytes

Parameters	Description
Free(%)	The percentage of total usable space on the disk that was free.
Free(MB)	The unallocated space on the disk in mega bytes.
Disk I/O Statistics	
Transfers/sec	The number of read/write operations on the disk that occur each second.
Writes/sec	The percentage of elapsed time that the disk drive was busy servicing write requests.
Reads/sec	The percentage of elapsed time that the disk drive was busy servicing read requests.
% Busy Time	The percentage of time the disk was busy.
Average Queue Length	The average number of both read and write requests that were queued for the disk during the sample interval.

You can also delete disks that have been physically removed using the **Delete Orphaned Disk** option.

Configuration

This tab contains information about system configuration attributes.

Parameters	Description
System Information	
Host Name	The name of the system.
Domain	The name of the domain to which the system belongs.
OS Information	
OS Name	The name of the operating system instance.
OS Version	Version number of the operating system.
OS Release	The Linux distribution
Memory Information	
Total Physical Memory (MB)	Total amount of physical memory as available to the operating system.
Total Swap Memory (MB)	Total amount of swap memory available.
Processor Information	
Id	Unique identifier of a processor on the system
Model	The processor model type

Parameters	Description
Implementation	The processor family type.
Manufacturer	Name of the processor manufacturer
Speed(MHz)	Current speed of the processor
Cache (KB)	Size of the processor cache. A cache is an external memory area that has a faster access time than the main memory.
Network Interface Settings	
Name	The name of the network adapter.
IP Address	The IP address configured for this network interface
MTU	The network medium in use.
Type	The type of network adapter.
Mac Address	The Media access control address for this network adapter. A MAC address is a unique 48-bit number assigned to the network adapter by the manufacturer. It uniquely identifies this network adapter and is used for mapping TCP/IP network communications.
Status	The current status of the network adapter.
Broadcast Address	The IP address to which messages are broadcast.
Printer Settings	
Name	Name of the printer.
Device	The name of the server that controls the printer.
Default	Indicates whether the printer is the default one. Values are either True or False.
Status	Current status of the printer.

Note: The data present in the configuration tab is not updated during every poll. So if you make any changes to the server configuration, you need to restart Applications Manager for those changes to be reflected in the 'Configuration' tab.

See Also

Creating New Linux Server Monitor

IBM AS400 / iSeries

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. In addition, it also provides the auxillary stroage pool percentage, processing unit percentage, number of users signed on and response time of the server. Each attribute has heat chart report enabled. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

The attributes for IBM AS400 / iSeries monitored are classified under the following tabs by Applications Manager:

- Overview
- Status
- Pool
- Jobs
- Messages
- Spool
- Printer
- Disk
- Problem
- Subsystem
- Admin

Overview

Parameters	Description
Monitor Information	This provides general information about the AS400/iSeries server such as name of the server, current health of the server, type, system model, system serial, and latest polled values. In addition, it also displays system configuration details such as security level, version number, Previous System End, Auto Device Configuration, System Console, Job Message Queue Initial Size, Job Message Queue Maximum Size, Spooling Control Initial Size, Maximum Jobs Allowed, Password Valid Days and Query Processing Time Limit.
Response Time	Displays the response time of the AS400/iSeries server.
Health	Provides the health of the server. It displays the Job health, Message health, Spool health, Printer health, Disk health, Problem health, and Subsystem health.

Parameters	Description
	<p>Job: Specifies the total number of user jobs and system jobs that are currently in the system. It also displays the performance and status information for the active jobs in the system.</p> <p>Message: Displays the total number of messages received from the server.</p> <p>Spool: Displays the output of the printer files in the server.</p> <p>Printer: Displays the number of printer devices connected to the server.</p> <p>Disk: Specifies the hard disk space utilized by the system.</p> <p>Problem: Displays the number of problems with ID and description from the server.</p> <p>Subsystem: Displays the total number of subsystems available under the server.</p>
Server Snapshot	<p>Server snapshot provides an quick overview of current server's auxillary storage pool's usage in percentage, processing units' usage in percentage, permanent address usage in percentage, temporary address usage in percentage and interactive performance usage in percentage.</p> <p>ASP Usage: The amount of hard disk capacity available in your system is called Auxiliary Storage Pool (ASP). This can be a deceiving number if you have more than one ASP defined on your system, because this number only reflects the System ASP. Applications Manager provides you with the percentage of disk storage in your System ASP that is currently used. If the percentage exceeds 90 percentage the system can fail. The performance of your AS400 server is affected if the percentage usage crosses 80 percent. You can create an alarm for this percentage and alert you whenever the percentage exceeds 80.</p> <p>Permanent addresses percentage and Temporary addresses Usage: Applications Manager provides you the usage in percentage for the two addresses - Permanent and Temporary Addresses - which refer to the possible system addresses created for permanent and temporary objects in your AS400. Any variation in these values may reflect on rapid changed in the creation or destruction of objects in your AS400 at much rapid pace. This may affect your performance of your server.</p>
Job Counts	<p>Provides the various job counts of various job types currently running in AS400/iSeries server. The information is displayed in a pie-chart with clearly distinction of each job types contribution to total job count. By default, the following services job count is displayed:</p> <ul style="list-style-type: none"> • Source PF system • Spooled Writer • System

Parameters	Description
	<ul style="list-style-type: none"> • Spooled Reader • Subsystem • Autostart • Interactive • Batch
System Information	System information displays the shared processing pool information, uncapped CPU utilization and current processing capacity resources.
Disk Utilization	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.)
Memory Utilization	Memory utilization for AS400/iSeries is displayed through pool size, reserved size, DB pages and Non DB pages and through DB faults and Non DB faults.

Status

Under **Status** tab, Applications Manager monitors the status of various attributes of AS400 / iSeries server. You can also configure alarms for each of these attributes by clicking on '**Configure Alarms**' link.

Parameters	Description
System Info	This contains details of your AS400 main storage, number of processors, number of pools, number of partitions and the number of active threads in your system along with the health of each individual attribute.
System Status	This displays the value and health of ASP percentage, DB percentage, Processing Unit percentage, Permanent and Temporary Addresses percentage.
ASP Percentage	The amount of hard disk capacity available in your system is called Auxiliary Storage Pool (ASP). This can be a deceiving number if you have more than one ASP defined on your system, because this number only reflects the System ASP. Applications Manager provides you with the percentage of disk storage in your System ASP that is currently used. If the percentage exceeds 90 percentage the system can fail. The performance of your AS400 server is affected if the percentage usage crosses 80 percent. You can create an alarm for this percentage and alert you whenever the percentage exceeds 80.
Auxillary Storage	The auxillary storage displays ASP total value and health, current unprotected useage and maximum protected usage along with the health of each attribute.

CPU Info	This displays the processing capacity, performance, shared processor pool and uncapped CPU capacity usage in percentages along with the health of each attribute.
Jobs	Displays the total number of jobs, number of active jobs, number of batch jobs, jobs waiting for messages, and maximum number of jobs in your AS400 server along with the health of each attribute. For number of active jobs, the 7/30 reporting is enabled.
Batch Jobs	Displays the number batch jobs ended, ending, held on queue and held while running along with the health of each attribute. It also displays the batch jobs on unassigned job queue and waiting to run/already scheduled jobs in AS400 server. For number of batch jobs on jobqueue, the 7/30 reporting is enabled.
Users	Displays the values for total number of users signed on and signed off, along with users suspended by group jobs, users suspended by system request and users temporarily signed off. For number of users signed on, the 7/30 reporting is enabled.

Pool

Under **Pool** tab, Applications Manager displays to pool details for the AS400 / iSeries server. Applications Manager provides you in-depth details for Pool such as Pool Name, Pool Size, DB pages, DB faults, Non DB pages and Non DB faults. The health and alarm configuration for each corresponding attribute is also provided.

Parameters	Description
Pool Name	<p>By default, there are four predefined storage pools:</p> <ul style="list-style-type: none"> *MACHINE *BASE *INTER and *SPOOL <p>There are up to 12 user-definable storage pools available.</p>
Pool Size	<p>This displays the amount of memory assigned to each default pools such as *MACHINE, *BASE, *INTER and *SPOOL. You can also edit the amount of memory allocated for each pool by executing the Change Subsystem Description (CHGSBSD) command through Non- interactive Command available in Admin tab. Better allocation would help improve the performance of the server.</p>

Parameters	Description
Reserved Size	This displays the pool's reserved memory allocation size. The information provided here gives better understanding to how much of the memory allocation has been used by jobs and how much memory is still unused. This reserved size can affect system performance. If insufficient memory is not provided to the default *MACHINE pool, then it can affect overall performance of your AS400 server. Hence monitoring this attribute becomes critical for maintaining better performance of your AS400 server.
DB and Non DB Faults and Pages	This displays the DB and Non DB pages and fault for each pool. This basically displays how program instructions and database information enter and leave the pool's memory. Monitoring this information provides better visibility on various programs and jobs that are being executed in AS400 server. Applications Manager allows you to monitor the various programs, data queues and configuration objects among others which lets you maintain the overall performance of AS400 server.

Jobs

Under **Jobs** tab, Applications Manager monitor Jobs status and health in detail. You can easily configure alarms for Job details by clicking on '**Configure Alarms**' link. The table consists of the following columns:

- Job Name
- User
- Number
- Type
- Status
- Pool
- Function
- Priority
- Threads and
- Queue

Parameters	Description
Job Details	Displays the total number of jobs in clear, critical and warning states along with the health of each attribute.
Jobs	Displays a wealth of information on various jobs being executed in AS400 server. Each attribute is explained below. Batch Job: The user name is specified on the Submit Job (SBMJOB) command,

Parameters	Description
	<p>or it is specified in the job description.</p> <p>Interactive Job: The user name is either typed in at signon or is provided by the default in the job description.</p> <p>Autostart Job: The user name is specified in the job description referred to by the job entry for the autostart job.</p>
Job Name	The name of the job as identified by AS400. This displays the total number of jobs executed in AS400 by the system and the total number of user initiated jobs in AS400.
User	The user name is the same as the user profile name and can come from several different sources, depending on the type of job.
Number	The system-assigned job number.
Type	<p>The type of active job. Possible values are:</p> <p>ASJ: Autostart</p> <p>BCH: Batch</p> <p>BCI: Batch Immediate</p> <p>EVK: Started by a procedure start request</p> <p>INT: Interactive o M36: Advanced 36 server job</p> <p>MRT: Multiple requester terminal</p> <p>PJ: Prestart job</p> <p>PDJ: Print driver job</p> <p>RDR: Reader</p> <p>SBS: Subsystem monitor</p> <p>SYS: System</p> <p>WTR: Writer Status</p>
Status	This displays the status of the initial thread of the job. Only one status is displayed per job. A blank status field represents an initial thread that is in transition.
Pool	This displays the system-related pool from which the job's main storage is allocated.
Function	This displays the last high-level function initiated by the initial thread. This field is blank when a logged function has not been performed. The field is not cleared when a function is completed.
Priority	This displays the run priority of the job. A lower number indicates a higher priority. System jobs and subsystem monitors with a run priority higher than priorities allowed for user jobs show a priority of 0. Run priority ranges from 1 (highest) to 99 (lowest). Jobs with the highest priority receive the best service from the CPU.

Parameters	Description
	This value is the highest run priority allowed for any thread within the job. Individual threads may have a lower priority.
Threads	Displays the number of active threads in the job.
Queue	Displays the name of the Queue where the job is located.

The job status in AS400/iSeries is classified into three types:

1. Jobs Clear
2. Jobs Warning
3. Jobs Critical

If you would like to define a particular job status as critical, edit *AS400server.properties* in AppManager Conf directory and include the particular job status as critical.

Open the conf file in the Applications Manager directory:

Windows: C:\Program Files\ManageEngine\<AppManagerHome>\conf


Linux: \ManageEngine\<AppManagerHome>\Conf

The file consists of jobs in pre-defined classification under clear, warning and critical categories. If you would like to include a particular job status say for example CMNA as critical, add CMNA in the following line as follows

am.as400.critical = MSGW, CMNA

Save the file and restart Applications Manager. After the next polling interval, you will find that the particular job is now classified as a Critical job status.

Messages

Message Information display gives you more detailed information about the various message(s) being displayed in your AS400 server. The messages are displayed with in-depth details such as message ID, severity of the message, type of the message, message text with a cause and recovery information if applicable, date and time of the message generated and help information for that particular message. You can view more detailed information of a particular message by clicking on the Help icon - .

Parameters	Description
Message ID	The message ID identifies the type of message. This is useful when doing problem analysis.
Severity	A 2-digit value ranging from 00 through 99. The higher the value the more severe or important the condition.
Type	<p>The following values may be shown:</p> <ul style="list-style-type: none"> • Completion: A message that conveys completion status of work. • Diagnostic: A message that indicates errors in a system function, errors in an application, or errors in input data. • Escape: A message that describes a condition for which a program must end abnormally. • Information: A message that provides general non error-related information. • Inquiry: A message that conveys information but also asks for a reply. • Notify: A message that describes a condition for which a program requires corrective action or a reply. • Reply: A message that is a response to a received inquiry or notify message. • Request: A message that contains a command for processing by a request processor, such as command entry. • Sender Copy: A copy of an inquiry or notify message that is kept in the sender's message queue.
Message	The text of the message.
Date	This is the date (in job format) that the message was sent.
Default Reply	Displays the default reply that was generated by your AS400 server for the particular generated message.
Help	<p>Displays in-depth details for the particular message from your AS400 server. It displays the following values:</p> <ul style="list-style-type: none"> • Message ID • Date Sent • Alert Option • Current User • From Job Number • From Program • Reply Status • File Name • Message • Cause

Top

228

Spool

Parameters	Description
Spool Name	The file name that was specified by the user program when the file was created, or the name of the device file used to create this file.
Number	The system-assigned spool number.
Job Name	The name of the job that produced the spooled file.
Job Number	The number of the job that produced this spooled file.
Job Owner	The name of the user who owns the spooled file.
Status	<p>The status of the spooled file. The following list of values is used to describe the file's status:</p> <p>RDY (Ready) The file is available to be written to an output device by a writer.</p> <p>OPN (Open) The file has not been completely processed and is not ready to be selected by a writer.</p> <p>DFR (Deferred) The file has been deferred from printing.</p> <p>SND (Sending) The file is being or has been sent to a remote system.</p> <p>CLO (Closed) The file has been completely processed by a program but SCHEDULE(*JOBEND) was specified and the job that produced the file has not yet finished.</p> <p>HLD (Held) The file has been held.</p> <p>SAV (Saved) The file has been written and then saved. This file will remain saved until it is released.</p> <p>WTR (Writer) This file is currently being produced by the writer on an output device.</p> <p>PND (Pending) The file is pending to be printed.</p> <p>PRT (Printing) The file has been completely sent to the printer but print complete status has not been sent back.</p> <p>MSGW (Message Waiting) This file has a message which needs a reply or an action to be taken.</p>
Pages	The total number of pages or records in the file (pages for print, records for diskette). If the file is still open, this field is blank for diskette files or will have the current number of pages spooled for printer files. An "R" is displayed after the value if the file is a diskette file.

[Top](#)

Printer

Parameters	Description
Device Name	Specifies the Printer or Device name.
Status	Specifies the status of the printer device. Valid values are 0 (varied off) 10 (vary off pending) 20 (vary on pending) 30 (varied on) 40 (connect pending) 60 (active) 66 (active writer) 70 (held) 75 (powered off) 80 (recovery pending) 90 (recovery canceled) 100 (failed) 106 (failed writer) 110 (being serviced) 111 (damaged) 112 (locked) 113 (unknown)
Job Name	Specifies the name of the job that created the spooled file.
Job Number	Specifies the number of the job that created the spooled file.
Job Owner	Specifies the name of the user that created the spooled file.
Total Pages	Specifies the number of pages that are contained in a spooled file.
Spooled File Name	Specifies the name of the spooled file.
Spooled File Number	Specifies the spooled file number. Special values allowed are -1 and 0. The value *LAST is encoded as -1, the value *ONLY is encoded as 0.
Spooled File Size	Specifies the spooled file size. Multiply this value by the spooled file size multiplier value to get the size of the spooled file in number of bytes. The spooled file size is the data stream plus the "overhead" storage used to store the spooled files's data stream.
Output Queue Name	Specifies the name of the output queue.
Output Queue Status	Specifies the status of the output queue. Valid values are RELEASED, HELD.

[Top](#)

Disk

The Disk Status display shows performance and status information about the disk units on the system. It displays the number of units currently on the system, the type of each disk unit, the size of disk space, whether the disk is currently on the system, the percentage of disk space used, the average amount of data read and written, and the percentage of time the disk is being used.

Parameters	Description
Disk Arm Number	Specifies the unique identifier of the unit. Each actuator arm on the disk drives available to the machine represents a unit of auxiliary storage. The value of the unit number is assigned by the system when the unit is allocated to an ASP.
Drive Capacity (in bytes)	Total number of bytes of auxiliary storage provided on the unit for the storage of objects and internal machine functions when the ASP containing it is not under checksum protection. The unit reserved system space value is subtracted from the unit capacity to calculate this capacity.
Drive Available Space (in bytes)	Total number of bytes of auxiliary storage space that is not currently assigned to objects or internal machine functions, and therefore is available on the unit.
Percentage of Use	The estimated percentage of time the disk unit is being used during the elapsed time. This estimate is based on the number of I/O requests, the amount of data transferred, and the performance characteristics of the type of disk unit. This field is blank if the performance characteristics of the disk unit are not available.
Blocks Write	Number of blocks written: The block length is 520 bytes, which includes 8 bytes of system control information.
Blocks Read	Number of blocks read: The block length is 520 bytes, which includes 8 bytes of system control information.
ASP	Specifies the ASP to which this unit is currently allocated. A value of 1 specifies the system ASP. A value from 2 through 32 specifies a basic ASP. A value from 33 to 255 specifies an independent ASP. A value of 0 indicates that this unit is currently not allocated.
Unit Status	Local mirroring status. 1 = active 2 = resuming 3 = suspended
Disk Wait Time	Combined wait (queue) time of all disk operations completed since last sample (milliseconds). Divide by number of read and write commands to obtain average wait (queue) time. Add to disk service time to obtain disk response time. Set to zero if data is not available.

Problem

Problem ID: Specifies the problem identifier of the problem being selected. Problems with different system origins can have the same identifier. This parameter can be used with the ORIGIN parameter to select a single problem from a particular system origin.

Problem Severity: This specifies the severity level of the problem. Severity levels are assigned by the user when the problem is prepared for reporting. The four severity levels are:

1. High
2. Medium
3. Low
4. None

Problem Type: Specifies which type of problems to work with. *ALL All problem log entries are shown, regardless of the problem type.

- 1 - Only machine-detected problems are shown.
- 2 - Only user-detected problems are shown.
- 3 - Only PTF order problems are shown.
- 4 - Only application-detected problems are shown.
- 5 - Only Client machine-detected problems are shown.
- 6 - Only Client user-detected problems are shown.

SubSystem

Name: The name of the subsystem that was specified on the STRSBS (Start Subsystem) command.

Current Active Jobs: The number of jobs active in the subsystem. If more than one interactive job is started from the same work station (with system request or Transfer to Group Job), they are counted as only one job on this display.

Status: The status of the subsystem, which can be either ACTIVE, END (in the process of ending), or RSTD (the controlling subsystem is in the restricted condition). More information on the restricted condition of the controlling subsystem is in the online help information for the ENDSBS command.

Library: The name of the library where the subsystem description is located. Maximum Active Jobs The maximum number of jobs active allowed in the subsystem.

Admin

Some of the key attributes on which certain actions can be performed are as given below.

Jobs - The following actions will be enabled for job attributes:

- END
- HOLD
- RELEASE

Messages - In messages you will be able to execute actions such as

- Remove
- Remove ALL
- Remove KEEP_UNANSWERED
- Remove NEW
- Remove OLD

Spool - In Spool, you will be able to execute the following actions:

- Delete
- Hold
- Release
- MoveToTop

Subsystem - In Subsystem, you will be able to execute the following actions:

- Delete
- End
- Start
- Refresh

In addition, you will be able to execute *Non-interactive commands* from Applications Manager and also will be able to edit any of the **System Value list** attributes.

See Also

Creating New IBM AS400 / iSeries Monitor

Virtualization

Applications Manager enables high performance business process management by detecting and diagnosing problems of virtualization infrastructure faster. Applications Manager supports the following virtual systems:

- VMWare ESX/ESXi Servers
- Hyper-V Servers
- Virtual Machines

See Also

Creating New Monitor - VMware ESX/ESXi Servers

VMware ESX/ESXi Servers

Supported Versions: ESX Server 3.5 and 4; ESX Server 3i

Monitored Parameters

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

The *Availability* tab shows the Availability history of the ESX server for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the ESX server such as CPU Utilization, Memory Utilization, Disk Usage and Network Usage along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* displays all the VMware ESX/ESXi servers along with an overall idea of their availability and health status. The list view also enables you to perform bulk admin configurations. Click on the individual servers listed to view detailed performance metrics.

The *Top ESX/ESXi* tab shows graphs for the top CPU consumers, top memory consumers, top disk I/O consumers and top network consumers of the ESX/ESXi server.

The *Infrastructure View* tab displays all the virtual machines discovered under each ESX/ESXi server. This view provides an overall idea of the availability, health, CPU (%), Memory (%), Disk I/O and Network traffic of all the virtual machines. Click on the individual virtual machines listed to view detailed VM metrics.

Click on the monitor listed in the *Availability* tab to view detailed performance metrics of the ESX/ESXi server. These metrics are categorized into 7 different tabs for easy understanding. Below is an explanation of the metrics shown in these tabs:

1) Overview

This tab provides a high-level overview of the ESX/ESXi server as well as its resource utilization.

Parameter	Description
Monitor Information	
Name	The name of VMware ESX/ESXi server monitor
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the ESX/ESXi server.

Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.
CPU & Memory Utilization	
CPU Utilization	The combined CPU utilization across the system(%)
CPU Usage	The total CPU usage across the system(MHz)
Memory Utilization	Percentage of memory used across the system(%)
Disk & Network Usage	
Disk Usage	Disk usage of ESX/ESXi server in kbps(kilobytes per second)
Network Usage	Network usage of ESX/ESXi server in kbps(kilobytes per second)
Virtual Machines	
VM Name	Name of the virtual machine(VM) present in the host
Availability	Denotes the availability of the VM - available or not available
CPU Utilization	The CPU utilization of this VM in percentage
Memory Utilization	The memory utilization of this VM in percentage
Disk I/O Utilization	The disk input/output utilization of this VM in kilobytes per second
Network Utilization	The network usage of this VM in kilobytes per second
Health	The health status(Clear, Warning, Critical) of this VM

2) CPU

This tab provides metrics about CPU Utilization details of the cores.

Parameter	Description
CPU Utilization	The cpu utilization of the CPU core over a period of time(in percentage)
Health	The overall health of the CPU core

3) Memory

This tab provides metrics about memory utilization of the ESX server.

Parameter	Description
Consumed Memory	The value of total memory minus free memory, in mega bytes.
Active Memory	Amount of memory that is actively used
Overhead Memory	Sum of overhead memory across all VMs
Reserved Memory	Amount of memory currently utilized to satisfy minimum memory values set for all VMs.
Shared Memory	Amount of memory shared between virtual machines
Granted Memory	Amount of physical memory granted
Swapped Memory	Amount of memory that is swapped
Heap Memory	Amount of memory allocated for heap
VMKernel Memory	Amount of memory used by the VMKernel

4) Datastore

This tab displays metrics pertaining to the data stores of the server.

Parameter	Description
Datastore	Name of the datastore
Type	Type of datastore (example: VMFS or VMware File System)
Capacity GB	The total space available in this datastore in giga bytes
Used GB	The used space of this datastore in giga bytes
Free GB	The free space of this datastore in giga bytes
Health	Overall health of the datastore

5) Network

This tab provides metrics about network utilization

Parameter	Description
Name	Name of the network interface card (NIC) of the host
Data Receive Rate	The rate at which this NIC receives data(Kbps)
Data Transfer Rate	The rate at which this NIC transfers data (Kbps)
Packets received	Number of network packets received by this NIC
Packets Transmitted	Number of network packets transmitted by this NIC
Health	Overall health of this NIC

6) Disk I/O

This tab shows detailed disk I/O(Input/Output) stats of the ESX/ESXi server

Parameter	Description
LUN	Logical unit number associated with the physical disk
Disk Read Rate	Disk read rate of this LUN(Kbps)
Disk Write Rate	Disk write rates of this LUN(Kbps)
Disk Reads	Number of reads to this LUN
Disk Writes	Number of writes to this LUN
Health	Overall health of this LUN

7) Configuration

This tab provides info on the ESX/ESXi server's configuration details.

Parameter	Description
Host Name	The name of VMware ESX/ESXi server monitor

Power	The power status of the server. The values include poweredOn, poweredOff and standBy
Vendor Name	The name of the vendor offering Virtualization(VMware)
Version	Version of ESX/ESXi server
Hardware Vendor Name	Hardware vendor identification
Hardware Model	System model identification
CPU Model	Information about the overall CPU
CPU Capacity MHz	The overall CPU capacity in Mega Hertz
CPU Cores	Number of CPU cores present in the server
Number of VMs	Number of virtual machines discovered in the server

See Also

Creating New Monitor - VMware ESX/ESXi Server

Virtual Machines

Monitored Parameters

The virtual machines (VMs) present in a VMware ESX/ESXi server are monitored based on the parameters or the attributes listed below. These attributes provide information about the functioning of the VMs. You can also configure thresholds to the numerical attributes of the VMs based on these details.

The Availability tab lists all the virtual machines present in the VSX/VSXi servers and their availability status. You can also view Availability history of the virtual machines for the past 24 hours or 30 days. The Performance tab shows some key performance indicators of the virtual machine including CPU Utilization, Memory Utilization, Disk I/O Utilization and Network Utilization along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The List view displays all the virtual machines discovered under each VSX/VSXi server. This view provides an overall idea of the availability and health of all the virtual machines. The list view also enables you to perform bulk admin configurations. Click on the individual virtual machines listed to view detailed VM metrics.

The Top Virtual Machines tab shows graphs for the top CPU consumers, top memory consumers, top disk I/O consumers, and top network consumers of the VSX/VSXi server. This section enables you to find out which virtual machines are consuming your server resources and take action accordingly.

Click on the individual monitors listed in the Availability tab to view detailed performance metrics of the corresponding virtual machine. These metrics are categorized into 6 separate tabs for easy understanding. Below is an explanation of the metrics shown in these tabs:

1) Overview

This tab provides a high-level overview of the virtual machine as well as its resource utilization.

Parameter	Description
Monitor Information	
Name	The name of the virtual machine
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the VM.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.

Availability	Shows the current status of the VM - available or not available.
CPU & Memory Utilization	
CPU Utilization	The CPU Usage of the VM as percentage
CPU Usage	The CPU usage in Mega Hertz
Memory Utilization	The memory utilization of the VM in percentage
Disk & Network Usage	
Disk I/O Utilization	The disk input/output utilization of the VM(kbps)
Network Utilization	The network usage of the VM in kbps

2) Memory

This tab shows metrics about the memory utilization of the virtual machine

Parameter	Description
Active Memory	Amount of memory that is actively used, measured as recently touched pages(MB)
Overhead Memory	Amount of additional host memory allocated to the virtual machine.
Swapped Memory	Amount of memory that is swapped.
Shared Memory	Amount of memory that is shared between virtual machines.
Ballooned Memory	Amount of memory held by memory control for ballooning.
Granted Memory	Amount of physical memory granted. For hosts this can be represented as regions of memory for each virtual machine.

3) Datastore

Parameter	Description
Datastore	Name of the datastore
Type	Type of datastore (example: VMFS or VMware File System)
Capacity GB	The total space available in this datastore in giga bytes
Used GB	The used space of this datastore in giga bytes
Free GB	The free space of this datastore in giga bytes
Health	Overall health of the datastore

4) Network

The metrics in this category contain the VM network status details.

Parameter	Description
Network Interface	
Name	Name of the Network Interface Card (NIC)
IP Address	The ip address of the NIC
Mac Address	The Mac address of the NIC
Network	The name of the network
Health	Indicates the health of the Network Interface Card
Network Interface Utilization	
Name	Name of the network interface card(NIC) of the host
Data Receive Rate	The rate at which this NIC receives data(KBps)
Data Transmit Rate	The rate at which this NIC transfers data (KBps)
Packets Received	Number of network packets received by this NIC
Packets Transmitted	Number of network packets transmitted by this NIC
Health	Overall health of this NIC

5) Disk I/O

This tab shows detailed disk I/O(Input/Output) stats of the virtual machine

Parameter	Description
LUN	Logical unit number associated with the physical disk
Disk Read Rate	Disk read rate of this LUN(KBps)
Disk Write Rate	Disk write rate of this LUN(KBps)
Disk Reads	Number of reads to this LUN during the defined interval
Disk Writes	Number of writes to this LUN during the defined interval
Health	Overall health of this LUN

6) Configuration

Parameter	Description
UUID	Universal Unique Identifier (UUID) assigned to the VM.
OS Name	Operating System assigned to the VM
Power	The status of the power of the virtual machine(poweredOn, poweredOff, suspend)

VM Path Name	Path name to the configuration file for the virtual machine, e.g. the .vmx file. This also implicitly defines the configuration directory.
IP Address	The IP address assigned to the VM
Host Name	The host on which the VM is running
Boot time	The time when the VM was booted.
Tools Version	Current version of VMware Tools running
Number of CPUs	Number of CPUs present in the VM
Configured Memory	The amount of memory configured for this VM
Number of Virtual Disks	The number of virtual disks in the VM

See Also

Creating New Monitor - VMware ESX/ESXi Server

Microsoft Hyper-V Servers

Supported Versions

Hyper-V Server 2008 R2, Windows Server 2008 R2 Standard, Windows Server 2008 R2 Enterprise, Windows Server 2008 R2 Datacenter

Monitored Parameters

Applications Manager monitors the critical components of the Hyper-V server to detect any performance problems. The components includes processor, memory, disk, virtual & physical network, virtual storage, etc.

The *Availability* tab shows the Availability history of the Hyper-V server for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the Hyper-V server such as Total CPU Utilization, Guest CPU Utilization, Hypervisor CPU Utilization and Physical Memory Utilization along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* lists all the Hyper-V servers monitored by Applications Manager along with their overall availability and health status. You can also perform bulk admin configurations from this view. Click on the individual servers listed to view detailed performance metrics.

The *Top Hyper-V servers* tab shows graphs for the top total CPU utilization consumers, top guest CPU utilization consumers, top memory consumers and top idle CPU utilization consumers.

To view detailed performance metrics of a Hyper-V server, click the corresponding monitor listed in the *Availability* or *List view* tab. These metrics are categorized into six different tabs for easy understanding.

Overview

This tab provides a high-level overview of the availability and performance of the Hyper-V server.

Parameter	Description
Monitor Information	
Name	The name of the Microsoft Hyper-V server monitor.
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the Hyper-V server.
Partitions	The total number of partitions in the Hyper-V server. Each virtual machine

Parameter	Description
	on the Hyper-V Server runs on a container called a partition.
Number of VMs	The number of virtual machines configured in this Hyper-V server (Partitions - 1)
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the server for the day. You can also view 7/30 reports and the current availability status of the server.
Hypervisor CPU Usage Details	
Total CPU Utilization	The sum of Guest CPU utilization and Hypervisor CPU utilization.
Guest CPU Utilization	The percentage of CPU used by guest VMs.
Hypervisor CPU Utilization	The percentage of CPU used by the hypervisor.
Idle CPU Utilization	The percentage of CPU when the processor is in an idle state.
Processor Details	
Logical Processors	The total number of logical processors present in the Hyper-V server. These are the number of cores / HT that the hypervisor is managing.
Virtual Processors	The total number of virtual processors present in the Hyper-V server. All execution in the root and child partitions (where guest VMs run) happens on Virtual Processors.
Physical Processors	The total number of physical processors present in the Hyper-V server.
Memory Details	
Total Physical Memory	The total amount of physical memory utilized by the Hyper-V system.
Total Swap Memory	The total swap space or the virtual memory utilized by the Hyper-V system.
Total Remote Physical Pages	The total number of physical pages not allocated from the preferred NUMA node.
Total Physical Pages Allocated	The total number of guest pages and VID pages needed to manage the VM.

Parameter	Description
HyperV System Services	
Service Name	The name of the system services of Hyper-V. The services available include Hyper-V Image Management Service, Hyper-V Networking Management Service and Hyper-V Virtual Machine Management.
Service Status	The current status of the service
Virtual Machines	
Virtual Machine	The name of the virtual machine.
VM State	Specifies the current state of the VM such as Running, Paused, Suspended, etc.
CPU Utilization	The percentage of CPU used by this VM
Total Memory	The amount of memory used by this VM
Health	Denotes the overall health status of the VM

Memory

This tab provides memory usage statistics of the Hyper-V server.

Parameter	Description
Memory Usage Details	
Swap Memory Utilization	The total swap memory or virtual memory used by the system in percentage
Swap Memory Used	The swap memory used by the system in mega bytes.
Physical Memory Utilization	The amount of physical memory used by the system in percentage.
Physical Memory Used	The amount of physical memory used by the system in mega bytes.
Free Physical Memory	The amount of free physical memory, in megabytes, immediately available for allocation to a process or for system use.
Page Details	
Deposited Pages	The total number of deposited pages used by the root partition.
Virtual TLB Pages	The total number of pages used by the virtual TLB of the root partition.

Parameter	Description
Total Remote Physical Pages	The number of physical pages not allocated from the preferred NUMA node.
Total Physical Pages Allocated	The total number of guest pages and VID pages needed to manage the VM.
Pages Per Second	The rate at which pages are read from or written to the disk to resolve hard page faults.

Network

This tab provides metrics about the overall networking performance of the Hyper-V server.

Parameter	Description
Network Traffic Stats	
Network Adapter Name	The name of the network adapter of the host.
Speed	The rate at which bytes are transferred in Mbps.
Input Traffic	The number of bytes received over the adapter in kilobytes per second.
Input Traffic Utilization	The percentage of input utilization.
Output Traffic	The number of bytes sent over the adapter in kilobytes per second.
Output Traffic Utilization	The percentage of output utilization.
Network Packet Stats	
Offloaded Connections	The number of TCP connections (over both IPv4 and IPv6) that are currently handled by the TCP chimney offload capable network adapter.
Outbound Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Outbound Packets Discarded	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent transmission. One possible reason for discarding packets could be to free up buffer space.
Packets Sent Per Second	The rate at which packets are send on the network interface
Packets Received Per Second	The rate at which packets are received on the network interface.

Storage

This tab displays metrics pertaining to the overall disk performance of the Hyper-V system.

Parameter	Description
Disk IO Details	
Name	The name of the storage device
Current Disk Queue Length	The number of requests outstanding on the disk at the time the performance data is collected.
Disk Bytes Per Second	The rate at which bytes are transferred to or from the disk during write or read operations.
Disk Transfers Per Second	The rate of read and write operations on the disk.
Disk Partition Details	
Free Space	The total usable space on the selected disk drive that is free.
Used Space	The total space on the disk currently in use.
Percent Used Space	The percentage of total space on the disk currently in use.
Percent Free Space	The percentage of total usable space on the selected disk drive that is free.

Virtual Storage

This tab provides information about the virtual storage devices of the Hyper-V server.

Parameter	Description
Virtual Storage Stats	
Name	The name of the virtual storage device.
Error Count	The total number of errors that have occurred on this virtual storage device.
Flush Count	The total number of flush operations that have occurred on this virtual storage device.
Read Count	The total number of read operations that have occurred on this virtual storage device.
Write Count	The total number of write operations that have occurred on this virtual storage device.

Parameter	Description
Read Bytes Per Second	The total number of bytes that have been read per second on this virtual storage device.
Write Bytes Per Second	The total number of bytes that have been written per second on this virtual storage device.
Virtual IDE Controller Details	
Name	The name of the virtual IDE controller.
Read Bytes Per Second	The number of bytes read per second from the disks attached to the IDE controller.
Read Sectors Per Second	The number of sectors read per second from the disks attached to the IDE controller.
Write Bytes Per Second	The number of bytes written per second to the disks attached to the IDE controller.
Written Sectors Per Second	The number of sectors written per second to the disks attached to the IDE controller.

Virtual Network

This tab shows detailed virtual network stats of the Hyper-V server.

Parameter	Description
Virtual Network Adapter Details	
Network Interface Name	The name of the virtual network interface configured in the Hyper-V
Bytes/Sec	The total number of bytes that have traversed the network adapter per second.
Packets/Sec	The total number of bytes received per second by the network adapter.
Legacy Virtual Network Adapter Details	
Legacy Network Interface Name	The name of the legacy network interface configured in the Hyper-V.
Bytes Received Per Second	The number of bytes received per second on the network adapter.
Bytes Sent Per Second	The number of bytes sent per second over the network adapter.

Parameter	Description
Bytes Dropped	The number of bytes dropped on the network adapter.
Virtual Switch Details	
Switch Name	The name of the virtual switch configured in the Hyper-V
Bytes Per Second	The total number of bytes per second traversing the virtual switch.
Packets Per Second	The total number of packets per second traversing the virtual switch.

You can enable, disable or delete virtual storage devices/VMs/network adapters/disk from Applications Manager itself. Just select the required item from the corresponding tab, and choose the appropriate action from the *Action* list box. You can also compare reports between any two metrics by using the 'Compare Reports' option.

See Also

Creating New Monitor - Microsoft Hyper-V Server

Hyper-V Virtual Machines

Monitored Parameters

Applications Manager monitors the virtual machines configured in the Hyper-V server. It gives the ability to manage VMs (Start/Stop/Restart) from the Applications Manager web client in case of any performance problems.

The *Availability* tab lists all the virtual machines present in the Hyper-V servers and their availability status. You can also view Availability history of the virtual machines for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the virtual machine including CPU Utilization, Memory Utilization, Disk I/O Utilization and Network Utilization along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* displays all the virtual machines discovered under each Hyper-V server. This view provides an overall idea of the availability and health of all the virtual machines. The list view also enables you to perform bulk admin configurations. Click on the individual virtual machines listed to view detailed VM metrics.

The *Top Virtual Machines* tab shows graphs for the top CPU consumers, top memory consumers, top disk I/O consumers, and top network consumers of the Hyper-V server. This section enables you to find out which virtual machines are consuming your server resources and take action accordingly.

Click on the individual monitors listed in the *Availability* tab to view detailed performance metrics of the corresponding virtual machine. Below is an explanation of the metrics shown in these tabs:

Parameter	Description
Monitor Information	
Name	The name of the virtual machine.
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the VM.
GUID	The unique Hyper-V identifier of this virtual machine.
VM State	Specifies the current state of the virtual machine.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the overall availability status of the VM for the day. You can also view 7/30 reports and the current availability status of the VM.

Parameter	Description
CPU Stats	
CPU Utilization	The CPU Usage of the VM as percentage
VM Details	
Number of Virtual Processors	The number of virtual processors present in the partition. All execution in this child partition happens on Virtual Processors.
Memory Details	
Total Memory	The total memory current available to the virtual machine, in mega bytes.
Deposited Pages	The number of deposited pages in this partition.
Address Spaces	The number of address spaces in the virtual TLB of the partition.
Virtual TLB Size recommended	The recommended number of pages to be deposited for the virtual TLB.
Virtual TLB Pages	The number of pages used by the virtual TLB of this partition.
GPA space modifications per second	The rate of modifications to the GPA space of this partition.
Virtual TLB Flush Entireties per second	The rate of flushes of the entire virtual TLB.
Physical Pages Allocated	The number of physical pages allocated in this partition.
Preferred NUMA Node Index	The preferred NUMA node index associated with this partition.
Remote Physical Pages	The number of physical pages not allocated from the preferred NUMA node.

See Also

Creating New Monitor - Microsoft Hyper-V Server

Cloud Apps

Cloud Applications

<space for introduction to cloud applications>

Applications Manager's monitoring capabilities enables you to ensure your cloud computing resources are performing as expected.

The following are the different server types supported by Applications Manager under the cloud apps category:

- Amazon EC2

Memcached Server

To create Amazon EC2 server monitor:

1. Click on **New Monitor** link.
2. Select **Memcached** under Cloud Computing/Virtualization category.
3. Specify the **Display Name** of the memcached server
4. Enter the **HostName** or **IP Address** of the host where Memcached server runs.
5. Enter the **Port** where the server is running.
6. If you want to enable Transaction test, select 'Yes' radio button, otherwise select 'No' button.
7. Set the **Polling Interval**.
8. Choose the **Monitor Group** with which you want to associate the Memcached server to, from the combo box (optional).
9. Click **Add Monitor(s)**. This discovers the Memcached server from the network and starts monitoring it.

See Also

Monitor Information - Cloud Apps | Create Other New Monitors

Amazon

Amazon Monitors

Applications Manager automatically discovers all the EC2 and RDS instances, and S3 buckets under your Amazon account. You can then enable monitoring for those instances and buckets as per your requirement.

Monitored Parameters

Amazon accounts are monitored based on the parameters or the attributes listed below. These attributes provide detailed information about the functioning of the Amazon account. You can also configure thresholds to the numerical attributes based on these details and get notified when the thresholds are violated.

The *Availability* tab shows the availability history of the Amazon account for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of the Amazon account such as Total EC2 Instances running and Total RDS Instances along with heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* displays all the Amazon instances along with an overall idea of their availability and health status. The list view also enables you to perform bulk admin configurations. Click on the individual applications listed to view detailed performance metrics.

Click on the monitor listed in the *Availability* tab to view detailed performance metrics of the Amazon instance. These metrics are categorized into 2 different tabs for easy understanding. Here is an explanation of the metrics shown in these tabs:

1) Instances

This tab provides a high-level overview of your Amazon account as well as information about the EC2 instances present in this account.

Parameter	Description
Monitor Information	
Name	The name of the Amazon account.
Type	Denotes the type you are monitoring.

Parameter	Description
Health	Denotes the health (Clear, Warning, Critical) status of the Amazon account.
Total EC2 Instances Running	The number of EC2 instances running in the account
Total EBS Volumes in use	The number of EBS storage volumes currently in use
Total RDS Instances	The total number of RDS instances present in the account
Last Polled at	Specifies the time at which the last poll was performed
Next Poll at	Specifies the time at which the next poll is scheduled
Today's Availability	Shows the overall availability status of the account for the day. You can also view 7/30 reports and the current availability status of the account
EC2 Instances	
Instance ID	The unique identifier of the EC2 instance
Region Name	The region where this EC2 instance is running
State	The current state of the instance. The values include <i>running</i> , <i>stopped</i> , <i>shutdown</i> and <i>terminated</i>
Platform	The OS on which the instance is running
Monitoring	Denotes whether CloudWatch monitoring is enabled for this instance.
Public DNS Name	The DNS name associated with the instance

You can perform the following admin actions on the EC2 instances:

Delete: Delete the EC2 instance from the account.

Assign Platform: Assign platforms such as Windows, Mac OS, etc. to instances

Enable CloudWatch: Option to enable CloudWatch monitoring for the instance.

Disable CloudWatch: Disable CloudWatch monitoring for the instance.

Start Instances: Option to start the EC2 instance from Applications Manager.

Stop Instances: Option to stop EC2 instances from Applications Manager

Reboot Instances: Option to reboot the EC2 instances from within Applications Manager.

2) RDS Instances

This tab provides details about the RDS Instances present in the Amazon account.

Parameter	Description
Instance ID	The unique identifier of the instance.
Region Name	The region in which the RDS instance is running
State	The current state of this instance. The possible values for this field are <i>available, creating, failed, rebooting, etc.</i>
DB Engine Name	The name of the database engine associated with this instance
Allocated Storage	The storage space allocated to this instance in Giga Bytes

3) S3 Buckets

This tab provides details about the S3 buckets present in the Amazon account.

Parameter	Description
Bucket Name	The unique name of the S3 bucket.
Bucket Size	The size of the S3 bucket in mega bytes.
Bucket Location	The geographical region where Amazon has stored this bucket. Regions currently supported by Amazon are US-Standard, US-West (Northern California), EU (Ireland) and APAC-Singapore.
Creation Time	The time when the bucket was created.
Virtual Folders	The number of folders present in this S3 bucket.
Number of Objects	The number of objects stored in this S3 bucket.

You can perform the following admin actions on the S3 buckets from within Applications Manager.

Disable: Disable the monitoring of S3 bucket.

Enable: Enable the monitoring of S3 bucket.

Delete: Delete the S3 bucket from Applications Manager. Use this option when S3 bucket is deleted from your Amazon account.

You can also view comparison reports based on attributes such as bucket size, virtual folders and number of objects.

See Also

[Creating New Monitor - Amazon](#)

Amazon EC2 Instances

Monitored Parameters

The Amazon EC2 instances are monitored based on the parameters or the attributes listed below. These attributes provide information about the functioning of the EC2 instances. You can also configure thresholds to the numerical attributes based on these details and get notified when the thresholds are violated.

The *Availability* tab shows the Availability history of the EC2 instances for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of an EC2 instance such as CPU Utilization, Volume Idle Time, Network In and Network Out along with the heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* displays all the EC2 instances present in the Amazon account along with an overall idea of their availability and health status. The list view also enables you to perform bulk admin configurations. Click on the individual instance listed to view detailed performance metrics.

Click on the monitor listed in the *Availability* tab to view detailed performance metrics of the EC2 instance. These metrics are categorized into 3 different tabs for easy understanding. Below is an explanation of the metrics shown in these tabs:

1) Overview

This tab provides a high-level overview of the EC2 instance as well as its performance indicators.

Parameter	Description
Monitor Information	
Name	The name of the EC2 instance
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the EC2 instance.
Region Name	Name of the region where the instance is running
Instance Type	Indicates the type of the EC2 instance
State	The current state of the instance. Valid values include running, stopped, shutdown and terminated
Public IP Address	The IP address of the instance.
Platform	Indicates the platform of the instance (eg: Windows)

Parameter	Description
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the instance for the day. You can also view 7/30 reports and the current availability status of the instance.
CPU Utilization	The CPU utilization of the instance
Network Traffic	
Network IN	Incoming traffic in bytes per minute
Network Out	Outgoing traffic in bytes per minute
Disk I/O	
Disk Read Ops	The average number of disk read operations per second.
Disk Write Ops	The average number of disk write operations per second.

2) Attached Volumes

This tab provides metrics about the EBS volumes attached to the EC2 instance.

Parameter	Description
Configuration	
Volume ID	The ID of the Amazon EBS volume. The volume and instance must be within the same Availability Zone and the instance must be running.
Size	The size of the volume in Giga Bytes.
Snapshot ID	Snapshot from which the volume was created.
Created Time	Time stamp when volume creation was initiated.
Attached Time	Time stamp when the attachment was initiated.
Delete on Termination	Specifies whether the Amazon EBS volume is deleted on instance termination.
Health	Denotes the health of the volume (clear, warning, critical)
Latency	

Parameter	Description
Idle Time	The time period when no read or write operations were waiting to be completed in percentage(%)
Write Latency	The average of the total number of seconds spent by all Write operations that completed in the period
Read Latency	The average of the total number of seconds spent by all Read operations that completed in the period
Volume Traffic	
Read Bandwidth	The sum of total number of Read operations in the period in bytes per second
Write Bandwidth	The sum of total number of write operations in the period in bytes per second
Volume IO	
Read Throughput	The sum of read operations in the period in seconds
Write Throughput	The sum of write operations in the period in seconds
Queue Length	The average number of read and write operation requests waiting to be completed over the period.

3) Configuration

This tab provides the configuration details of the EC2 instance.

Parameter	Description
Instance ID	The unique key that identifies the EC2 instance.
Instance Type	Indicates the type of the instance.
Instance Launch Time	The time at which the instance was launched
State	The current state of the instance. The values include running, stopped, shutdown and terminated
Image ID	Image ID of the AMI used to launch the instance.
AMILaunch Index	The AMI launch index, which can be used to find this instance within the launch group.

Parameter	Description
Public DNS Name	The public DNS name assigned to the instance. This DNS name is contactable from outside the Amazon EC2 network.
Private DNS Name	The private DNS name assigned to the instance. This DNS name can only be used inside the Amazon EC2 network.
Public IP Address	The IP address of the instance.
Private IP Address	The private IP address assigned to the instance.
KeyPair Name	The name of the key pair, if this instance was launched with an associated key pair.
Platform	Indicates the platform of the instance (eg: Windows)
Availability Zone	The instance's availability zone.
Architecture	The architecture of the image.
RamDisk Id	RAM disk associated with this instance.
Kernel Id	Kernel associated with this instance.
RootDevice Type	The root device type used by the AMI. The AMI can use an Amazon EBS or instance store root device.
RootDevice Name	The name of the root device used by the AMI.
Monitoring	Indicates whether monitoring is enabled for the instance.

See Also

Creating New Monitor - Amazon

Amazon RDS Instances

Monitored Parameters

Amazon RDS Instances are monitored based on the parameters or the attributes listed below. These attributes provide information about the functioning of the RDS instance. You can also configure thresholds to the numerical attributes based on these details and get notified when the thresholds are violated.

The *Availability* tab shows the Availability history of the RDS instances for the past 24 hours or 30 days. The *Performance* tab shows some key performance indicators of an EC2 instance such as CPU Utilization, Free Storage Space, Database Connections and Write Throughput along with the heat charts for these attributes. This tab also shows the health status and events for the past 24 hours or 30 days.

The *List view* displays all the RDS instances present in the Amazon account along with an overall idea of their availability and health status. The list view also enables you to perform bulk admin configurations. Click on the individual instance listed to view detailed performance metrics.

Click on the monitor listed in the *Availability* tab to view detailed performance metrics of the RDS instance. These metrics are categorized into 2 different tabs for easy understanding. Below is an explanation of the metrics shown in these tabs:

1) Overview

This tab provides a high-level overview of the RDS Instance as well as its resource utilization.

Parameter	Description
Monitor Information	
Name	The name of the RDS instance.
Type	Denotes the type you are monitoring.
Health	Denotes the health (Clear, Warning, Critical) status of the RDS instance.
Region Name	The region in which the RDS instance is running.
Instance Type	Indicates the type of instance
Created Time	The time when the instance was created.
State	The current state of the instance. The values include running, stopped, shutdown and terminated

Parameter	Description
DB Engine Name	The name of the database engine associated with this instance
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Today's Availability	Shows the overall availability status of the instance for the day. You can also view 7/30 reports and the current availability status of the instance.
CPU Utilization	
CPU Utilization	The percentage of CPU Utilization
Free Storage Space	The amount of available storage space.
Database Connections	The number of database connections in use.
Network Traffic	
Read Throughput	The average number of bytes read from the disk per second.
Write Throughput	The average number of bytes written to the disk per second.
Network Latency	
Read Latency	The average amount of time taken per disk read operation.
Write Latency	The average amount of time taken per disk write operation.
Disk I/O	
Read Ops	The average number of disk Read operations per second.
Write Ops	The average number of disk write operations per second.

2) Configuration

This tab provides the configuration details of the RDS instance.

Parameter	Description
Instance ID	The unique key that identifies the RDS instance
Instance Type	Indicates the type of instance
Created Time	The time when the instance was created.
State	The current status of the instance. Valid values include available, backing-up, creating, deleted, deleting, failed, modifying, rebooting and resetting-master-credentials

Parameter	Description
DB Engine Name	The name of the database engine used for this instance.
MasterUser Name	The master username for the instance.
DB Name	Name of the initial database created when the instance was created.
Allocated Storage	The storage space initially allocated to this instance, specified in GBs
Endpoint Address	The DNS Address of the DB instance
Endpoint Port	Port used to connect to the DB instance
Multi(A-Z)Deployment	Indicates if this is a Multi-AZ DB Instance.
Availability Zone	The instance's availability zone
PreferredBackup Window	The daily period during which automated backups are created.
LatestRestorableTime	The latest time to which a database can be restored using point-in-time restore.
BackupRetentionPeriod	The number of days that automated backups are retained before deletion.
PreferredMaintenanceWindow	The period during which patching and instance modifications will be performed.

See Also

Creating New Monitor - Amazon

Services

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

- JMX Applications
- Ping Monitor
- Service Monitoring
- SNMP
- Telnet
- Active Directory
- DNS Monitor
- FTP/SFTP Monitor
- LDAP Monitor

It performs the following checks to ensure its availability and represents the information in the form of graphs. *Availability* tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Service Type	Checks
JMX Applications	<ul style="list-style-type: none"> • 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, alarms can be generated for JMX notifications through JMX Notification Listener. For information on adding Custom Monitors, refer to Custom Monitors topic.
Ping Monitor	<ul style="list-style-type: none"> • Applications Manager uses Ping Monitor to track if the particular host / IP address is accessible or not. It checks for availability of a device, server or network device • The parameters that are monitored are • Packet Statistics: • Packet Loss (%): Packet loss gives the percentage of packets that fail to reach the destination. Packets Sent: No. of Packets sent. Packet Received: No. of Packets received. • Round Trip Time: Time taken for each packet exchange. Ping places a timestamp in each packet, which is echoed back and is used to compute how long each packet exchange took

Service Type	Checks
Service Monitoring	<ul style="list-style-type: none"> 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.
SNMP	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Connects to Telnet port (default 23) and checks its availability. Monitors response time and updates the status based on a given threshold.
DNS Monitor	<ul style="list-style-type: none"> Monitors the availability and performance of DNS monitors. It also monitors individual attribute of DNS monitor such as Response Time, Record Type, Record Available, Search Field, Search Value, Search Value Status and Search Time.
FTP/SFTP Monitor	<p>Monitors the availability and performance of FTP/SFTP monitor. In addition, it monitors Connection Time, Login Time, File Transfer, File Transfer Speed, Full Transaction and Files & Directories located in the Home Directory.</p> <p>Connection Time: Time taken by Applications Manager to connect to FTP server.</p> <p>Login Time: Time taken by Applications Manager to login to FTP server.</p> <p>File Transfer: It is the time taken for a file to either upload (mput) or download (mget) to a FTP server. In addition, the file size is also monitored while being uploaded or downloaded.</p> <p>File Transfer Speed: It is the time taken by a particular file transferred to (mput) or from (mget) a FTP server.</p> <p>Full Transaction: This provides the number of uploads/downloads that was completed correctly.</p> <p>Files & Directory (Home Directory): This provides the number of files and directories that were present in the FTP server.</p>

Service Type	Checks
LDAP Monitor	<p>Monitors the availability and performance of LDAP server. It monitors the Login Time attribute - the time taken for a user to log in to the LDAP server. In addition, it also monitors Search Details and Search Results Details.</p> <p>The 'Search Details' section displays the time taken for a search to execute and the total response time. The total response time is the login time plus the time taken for a search in the LDAP server.</p> <p>The 'Search Results Details' displays the search result row count which displays the total rows returned after a search was executed and the search result matching details which displays whether it was a success or a failure.</p>

Active Directory Monitor: Connects to the Active Directory server and checks its **availability**. Active Directory Counters that are monitored by Applications Manager are given below.

Parameters	Description
Network Monitors	
AB Client Sessions	AB Client Sessions is the number of connected Address Book client sessions.
DS Notify Queue Size	The number of pending update notifications that have been queued, but not yet transmitted to clients
Database Monitors	
Database Disk Free Space	Shows the percentage of the total usable space on the selected logical disk drive that was free
Database File Size	Shows the DataFile Size in bytes.
Database Disk Total Size	Shows the Total Size of the disk drive
NTFRS Process Monitors	
NTFRS CPU Usage	Percentage of elapsed time that all of the threads of NTFRS process used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions is included in this count.

Parameters	Description
NTFRS Handle Count	Total number of handles the NTFRS process has open. This number is the sum of the handles currently open by each thread in the process.
NTFRS Process File Reads	Rate at which the NTFRS process is reading bytes from I/O operations. This property counts all I/O activity generated by the NTFRS process to include file, network, and device I/Os.
NTFRS Process File Writes	Rate at which the NTFRS process is writing bytes to I/O operations. This property counts all I/O activity generated by the NTFRS process to include file, network, and device I/Os
NTFRS Process Memory	Amount of memory in bytes that a NTFRS process needs to execute efficiently—for an operating system that uses page-based memory management. If the system does not have enough memory (less than the working set size), thrashing occurs. If the size of the working set is not known, use NULL or 0 (zero).
System Monitors	
CPU Utilization	Percentage of time that the processor is executing a non-idle thread. This property was designed as a primary indicator of processor activity. It is calculated by measuring the time that the processor spends executing the thread of the idle process in each sample interval and subtracting that value from 100%.
Disk Utilization	It is calculated as follows $((\text{size} - \text{free size}) / \text{size}) * 100$ where size-----It is the total Size of the disk drive on Logical Disk free size---Space, in bytes, available on the logical disk
Memory Utilization	It is calculated as follows $((\text{TotalVisibleMemorySize} - \text{FreePhysicalMemory}) / \text{TotalVisibleMemorySize}) * 100$ where TotalVisibleMemorySize- Total amount, in kilobytes, of physical memory available to the operating system. This value does not necessarily indicate the true amount of physical memory, but what is reported to the operating system as available to it. FreePhysicalMemory- Number, in kilobytes, of physical memory currently unused and available.
Number of Processes	Number of process contexts currently loaded or running on the operating system.
OS Processor Queue Length	Number of threads in the processor queue. There is a single queue for processor time even on computers with multiple processors. Unlike the disk counters, this property counts ready threads only, not threads that are running.

Parameters	Description
Performance Counter Monitors	
DS Client Binds	Shows the number of Ntdsapi.dll binds per second serviced by this domain controller.
DS Server Binds Per Sec	Shows the number of domain controller-to-domain controller binds per second that are serviced by this domain controller.
Directory Reads Per Sec	Shows the number of directory reads per second.
Directory Writes Per Sec	Shows the number of directory writes per second.
NTLM Authentications	Shows the number of NTLM authentications per second serviced by this domain controller.
Kerberos Authentications	Shows the number of times per second that clients use a ticket to this domain controller to authenticate to this domain controller.
LSASS Process Monitors	
LSASS CPU Usage	Percentage of elapsed time that all of the threads of LSASS process used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions is included in this count.
LSASS Handle Count	Total number of handles the LSASS process has open. This number is the sum of the handles currently open by each thread in the LSASS process.
LSASS Process File Reads	Rate at which the LSASS process is reading bytes from I/O operations. This property counts all I/O activity generated by the LSASS process to include file, network, and device I/Os.
LSASS Process File Writes	Rate at which the LSASS process is writing bytes to I/O operations. This property counts all I/O activity generated by the LSASS process to include file, network, and device I/Os
LSASS Process Memory	Amount of memory in bytes that a LSASS process needs to execute efficiently—for an operating system that uses page-based memory management. If the system does not have enough memory (less than the working set size), thrashing occurs. If the size of the working set is not known, use NULL or 0 (zero).

Parameters	Description
LDAP Stats	
LDAP Active Threads	Shows the current number of threads in use by the LDAP subsystem of the local directory service.
LDAP Bind Time	Shows the time, in milliseconds, taken for the last successful LDAP bind.
LDAP Client Sessions	Shows the number of currently connected LDAP client sessions
LDAP Searches Per Sec	Shows the rate at which LDAP clients perform search operations
LDAP UDP operations Per Sec	Shows the number of User Datagram Protocol (UDP) operations that the LDAP server is processing per second.
LDAP Writes Per Sec	Shows the rate at which LDAP clients perform write operations.
Replication Stats	
Replication Objects Applied Per Sec	Shows the rate at which replication updates received from replication partners are applied by the local directory service. This counter excludes changes that are received but not applied
Replication Objects Remaining	Shows the number of object updates received in the current directory replication update packet that have not yet been applied to the local server.
Total Replication Objects In /Sec	Shows the number of objects received from neighbors through inbound replication. A neighbor is a domain controller from which the local domain controller replicates locally.
Total Replication Objects Out /Sec	Shows the number of objects replicated out.
Replication Traffic In	Shows the total number of bytes replicated in. This counter is the sum of the number of uncompressed bytes (never compressed) and the number of compressed bytes (after compression).
Replication Traffic Out	Shows the total number of bytes replicated out. This counter is the sum of the number of uncompressed bytes (never compressed) and the number of compressed bytes (after compression)

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

Mail Servers

Applications Manager supports monitoring of the following Mail Servers

- Exchange Server [2003 | 2007 | 2010]
- Mail Server

It performs the following checks to ensure its availability and represents the information in the form of graphs. *Availability* tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Exchange Server 2003

- 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:

SMTP Connections	Inbound Connections Outbound Connections
Message Transfer Agent Connections	Inbound Associations Outbound Associations
POP & IMAP Connections	POP Connections IMAP Connections
Information Store Connections & Users	Active Connections Active Users
SMTP Stats	Local Retry Queue Length Remote Retry Queue Length

	Remote Queue Length Messages Pending Routing Messages in Local Delivery Currently Undeliverable Messages Categorizer Queue Length
MTA Stats	Work Queue Length Message Bytes Per Sec TCP/IP Received Bytes Per sec TCP/IP Transmit Bytes Per sec Total Recipients Queued Work Queue Bytes Queue Length Queued Bytes
Information Store Stats	Messages from MTA to IS Messages from IS to MTA Messages Pending Local Delivery Messages Received Per sec Messages Sent Per sec HSOT Cache Hits
Information Store Mailbox Stats	Receive Queue Size Send Queue Size Messages Delivered Per min Messages Sent Per min Logon Operations Per sec Used Disk Space
Directory & Event Service Stats	Pending Replication Synchronizations Remaining Replication Updates Notify Queue AddressLists Queue Length
Information Store Public Folder Stats	Receive Queue Size Send Queue Size Messages Delivered Per min Messages Sent Per min Logon Operations Per sec Used Disk Space

Exchange Server 2007

- 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 Active Directory Topology
 - MS Exchange Anti-spam Update
 - MS Exchange EdgeSync
 - MS Exchange File Distribution
 - MS Exchange Mailbox Assistants
 - POP3
 - IMAP4
 - MS Exchange Information Store
 - MS Exchange Mail Submission
 - MS Exchange Monitoring
 - MS Exchange Replication Service
 - MS Exchange System Attendant
 - MS Exchange Search Indexer
 - MS Exchange Service Host
 - MS Exchange Transport
 - MS Exchange Transport Log Search
 - MS Exchange ADAM
 - MS Exchange Credential Service
 - MS Exchange Speech Engine
 - MS Exchange Unified
 - Messaging MS Search (Exchange)
- 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:

SMTP Connections	Inbound Connections
	Outbound Connections
	Messages Sent Per second
	Messages Received Per second
POP & IMAP Connections	POP Connections
	IMAP Connections
Transport Queue Stats	Active Mailbox Delivery Queue Length
	Retry Mailbox Delivery Queue Length
	Retry Remote Delivery Queue Length
	Messages Queued for Delivery Per Second
	Messages Submitted Per Second
	Items Queued For Delivery Per Second

Cache Stats	No. of Cache Active Connections No. of Cache Idle Connections No. of Cache Connections Cache Total Capacity RPC Requests Sent Per Seconds RPC Requests Outstanding RPC Latency Average ms
Availability Stats	Availability Requests Per Second Mailbox Session Hits Public Folder Queries Per Second Public Folder Request Failures Per Second
Active Directory Access Stats	Cache Hits Per Second Cache Misses Per Second LDAP Searches Per Second Outstanding Asynchronous Reads

Exchange Server 2010

- Connects to system in which Exchange Server 2010 is running, to check **availability** of the Exchange Server. Checks for the availability of the following services:
 - MS Exchange Active Directory Topology
 - MS Exchange Anti-spam Update
 - MS Exchange EdgeSync
 - MS Exchange File Distribution
 - MS Exchange Mailbox Assistants
 - POP3
 - IMAP4
 - MS Exchange Information Store
 - MS Exchange Mail Submission
 - MS Exchange Monitoring
 - MS Exchange Replication Service
 - MS Exchange System Attendant
 - MS Exchange Search Indexer
 - MS Exchange Service Host
 - MS Exchange Transport
 - MS Exchange Transport Log Search
 - MS Exchange ADAM
 - MS Exchange Credential Service
 - MS Exchange Speech Engine
 - MS Exchange Unified
 - Messaging MS Search (Exchange)

- 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:

SMTP Connections	Inbound Connections Outbound Connections Messages Sent Per second Messages Received Per second
POP & IMAP Connections	POP Connections IMAP Connections
Transport Queue Stats	Active Mailbox Delivery Queue Length Retry Mailbox Delivery Queue Length Retry Remote Delivery Queue Length Messages Queued for Delivery Per Second Messages Submitted Per Second Items Queued For Delivery Per Second
Cache Stats	No. of Cache Active Connections No. of Cache Idle Connections No. of Cache Connections Cache Total Capacity RPC Requests Sent Per Seconds RPC Requests Outstanding RPC Latency Average ms
Availability Stats	Availability Requests Per Second Mailbox Session Hits Public Folder Queries Per Second Public Folder Request Failures Per Second
Active Directory Access Stats	Cache Hits Per Second Cache Misses Per Second LDAP Searches Per Second Outstanding Asynchronous Reads

Mail Server

- Connects to the Mail Server and performs both SMTP and POP operations, by sending and fetching test mails.
- 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 Server / Services

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

- Apache Server
- IIS Server
- Real Browser Monitor
- PHP
- SSL Certificate Monitor
- Web Server
- Web Services
- HTTP - URLs and HTTP - URL Sequence (Record and Playback)

It performs the following checks to ensure its availability and represents the information in the form of graphs. *Availability* tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Service Type	Checks
Apache Server	<p>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.</p> <ol style="list-style-type: none"> 1. Total Accesses 2. Total KBs 3. CPU Load 4. ReqPerSec 5. BytesPerSec 6. BytesPerReq 7. BusyWorkers 8. IdleWorkers <p>To Enable the Server Status, follow the steps given below:</p> <ol style="list-style-type: none"> 1. In Apache's httpd.conf file, locate "Location /server-status" tag. If you are not able to locate the server-status tag, do the following 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".

Service Type	Checks
	<p>5. Save the conf file and restart the Apache Server</p> <p>To enable the Extended-status, follow the steps given below:</p> <ol style="list-style-type: none"> 1. Locate "ExtendedStatus" Attribute in httpd.conf file. 2. Remove the comment to enable the status. 3. Save the conf file and restart the Apache Server <p>Note : For Apache 2.2.3 and above, make the following changes in the /opt/apache-httpd-2.2.3/conf/httpd.conf file.</p> <p>Add the following lines at the end of the file,</p> <pre><Location /server-status> SetHandler server-status Order deny,allow Deny from all Allow from all </Location> ExtendedStatus On</pre> <p>Then restart the Apache server, try to connect to http://<your.server.name>/server-status and then you should be able to view the server status.</p>
IIS Server	<ul style="list-style-type: none"> • Connects to the IIS server and checks its availability. • Monitors response time and updates the status based on a given threshold. • If the host in which IIS server is running is monitored in WMI mode, the website stats can also be monitored. Health of the IIS Server depends upon the health of the websites. Health of the Website depends upon attributes that are mentioned below. • Bytes Transferred : Bytes Sent Per Second, Bytes Received per Second, Bytes Total Per Second • Files Transferred: Files Sent Per sec, Files Received Per sec, Files Transferred Per Sec • Connection Statistics: Current Connections • Anonymous Users: Current Anonymous Users, Anonymous Users per Second • Non Anonymous Users: Current NonAnonymous Users, Non Anonymous Users per Second
PHP Monitoring	<ul style="list-style-type: none"> • Connects to the server and retrieves PHP and checks its availability. • Monitors response time and updates the status based on a given threshold. • In Linux, Page fault of the system in which the PHP is hosted is also shown. We can configure the alarm and actions based on the threshold condition..
SSL Certificate	<ul style="list-style-type: none"> • Connects to the server and retrieves the details pertaining to the validity and authenticity of the SSL Certificate.

Service Type	Checks
Monitoring	<ul style="list-style-type: none"> • Monitors the availability and response time of the domain being added. • Issued To: Displays the details of the organization for which the certificate is issued. • Issued By: Displays the details about the Certification Authority of your domain. • Validity: Specifies details such as the issue date and expiry date of the SSL Certificate and also the number of days left for expiry. • Threshold can be set to configure alarms which will alert you before your certificate expires.
Web Server	Connects to the web server and checks its availability. Monitors response time and updates the status based on a given threshold.
Web Service	Connects to the web service and checks its availability. Monitors WSDL URL response time and updates the status based on a given threshold. Monitors Web Service Operation Execution time

Web Service Monitoring

Web Services is an XML-based technology that allow applications to communicate with each other, regardless of the environment, by exchanging messages in a standardized format (XML) via web interfaces (**SOAP** and **WSDL APIs**).

ManageEngine Applications Manager provides a flexible approach to manage a SOA that uses SOAP Web Services. It helps business managers configure SLAs and track high level availability of the Web Service. Application admins can monitor the performance of these Web Services by configuring Applications Manager to execute 'Operations' published by the Web Service. By specifying the WSDL, a simple wizard helps you configure operations that need to be invoked and gives the ability to specify arguments to the operation. In addition to this, there is out-of-the-box support for configuring thresholds on individual operation execution times and taking corrective actions.

Adding Operations

You can add Operations to the Web Service for monitoring. Operations are abstract descriptions of actions supported by the service.


Follow the steps given below to add operations:

1. Click the **Add Operation** link present on the right-hand side of the web services monitor screen. This displays the Add Operation screen.
2. The operations configured in the web service will be listed in the **Select Operation** drop-down list box. You can either choose any of these operations or choose custom operation.

3. If you select a pre-configured operation, the **SOAP Action** and **SOAP Request** values for the operation will be automatically displayed. Replace the '?' in the SOAP request with your input value.
4. If you choose the custom operation, you have to specify the Operation Name, SOAP Action and SOAP Request values.
5. You can use the **Test Operation** option to check the output before adding the operation for monitoring.
6. Click **Save** button to add the operation. Click **Save and Configure Another** button to add the operation and configure another operation.

The Operations thus added, will be listed in the details page under the **Operation Statistics** section. In this section, you can view the details of the operation such as Operation Name, SOAP Request, SOAP Response, status and execution time. You can also configure thresholds and alarms for all the operations.

Editing Arguments

Click the **Manage Operation** link under the 'Operation Statistics' section to go to the 'Manage Operation' page. In this page, click the  icon to edit the **Operation Display name** as well as the **Arguments** including SOAP Action and SOAP Request values.

You can also enable/disable reports for the operations from the *Manage Operation* page. If you disable reports, Applications Manager will not update the Operation Execution Time graph for that time period.

See Also

Creating New Monitor - Web Server / Services

Real Browser Monitor

Real Browser Monitor (RBM) provides live End-User experience measurement. RBM opens up a Microsoft Internet Explorer Browser and monitors a web application just like how a real user sees it. It supports playback from different geographical locations.

For eg., if you have different users logging in to your application from UK, US, Germany, Australia, etc. you can monitor their experience from a central Applications Manager Server. You could have the Applications Manager running in a data center in India and have the Real Browser Monitor agents deployed in other geographical locations and have it report Web Application Performance data to the central site. This way you can monitor the availability and performance of the website pages at different locations.

Working of Real Browser Monitor

- Components of RBM - **Toolbar** for Browser (Internet Explorer), **EUM agent** to be installed from where the "Internet Explorer" playback has to be performed and **Applications Manager Server**.
- End User Monitoring(EUM) agents (separate .exe downloads) need to be installed in the client locations.
- **System requirement** for the machine where EUM agent is to be deployed :
EUM agents have to be installed on a dedicated Windows Machine - 256 MB RAM, 1 GB HD, with Internet Explorer 6 or above. However, Applications Manager can be installed on Windows or Linux. This works with the Professional Edition and Enterprise Edition (with Managed Server).
- EUM agents register to ManageEngine Applications Manager on startup. You need to specify the "host and Web Client Port" of Applications Manager the first time the agent is installed and running. The agents get listed automatically.
- Using the RBM Toolbar you can record the required URL sequences and the actions that a typical end-user would access. The actions will be recorded as webscripts. The webscripts can be viewed in the webscript manager.
- Real Browser monitor is created in Applications Manager server by calling the required webscripts and agents. The EUM agent will periodically check Applications Manager Server if RBM monitor has been configured for this agent. If available, the EUM agent will run the webscript associated, by invoking Internet Explorer. The recorded actions will be replayed in the browser. **[Note: While playback is happening, do not close the Internet Explorer]**. Once the playback is complete, EUM agent will update the results of the playback [response time, response code, etc] in Applications Manager.

Only one Internet Explorer used by EUM agent can run in the background / foreground while playback is in progress. This means only one transaction can be executing at a time.

Applications Manager takes care of ensuring this synchronized playback.

- The availability and performance of the websites are monitored in real time by using the Real Browser monitor. If the health of the URLs is critical, then alarms can be generated. Based on the alarms, the admin will fix the issue.

Monitoring End-User Experience with RBM Monitor

The availability and response time of the recorded URLs will be monitored according to the poll interval set. Alarms are configured based on threshold configurations. So, if the health of the URLs is critical, alarms will be generated.

The *Availability* tab gives the Availability history for the past 24 hours or 30 days. The *Performance* tab gives the Health history for the past 24 hours or 30 days and also the Total Response Time of the various monitors. The *List* view enables you to perform bulk admin configurations. Click on the individual monitors listed to view the following information:

Monitor Information

Parameter	Description
Name	Denotes the name Real Browser Monitor
Health	Denotes the health (Clear, Warning, Critical) of the monitor based on its dependencies.
Polling Interval	Time set for the polling interval
Agent	Name of the EUM agent
Script	Name of the Webscript
Availability	The current status of the monitor - whether up or down
Validation	Results of the functions - Content Check, Element check will be updated for each URL. Content Check - You can validate a specific content in the page. Element Check - You can validate a specific element like Hyperlink in the page.

Performance - Last One hour

Parameter	Description
Average Response Time	The average response time for accessing an URL or total average response time of the URL Sequence (takes into account the avg.response time of the individual URLs in the Sequence)
Current Response Time	The current response time of the individual URL or the entire URL Sequence

PageSize - Last One Hour

Parameter	Description
Current Page Size	The current page size of the URL in bytes
% Page Size Change	The percentage change in current page size when compared to previous page size
Previous Page Size	The page size of URL in the previous poll

RBM Dashboard

The RBM dashboard provides an overview of the status of your webscripts or transactions from multiple locations. If you click on the individual scripts listed, it will take you to a page which shows the following metrics:

- **Total response time of the transaction across each location(agent):**
 - This section provides a graphical representation of the total response time of the transaction across the different locations where the webscript is running.
- **Current status and response time of the transaction across each location:**
 - This section provides a tabular representation of the current status and response time (in milliseconds) of the webscript from the locations where the script is running. The location showing maximum response time will be highlighted on the page. This indicates you the location from where the transaction is responding slow.
- **Total response time of the individual urls in the transaction:**
 - This section provides a good indication of how each individual url present within a transaction performs from different geographical locations. This section lists all the urls of the transaction and shows the response time of each url from multiple locations. The location from which the url has the maximum response time value will be highlighted. Click on any of the response time values listed to navigate to the 'Monitor Information' page of that particular url.

FAQ:

1. How does Real Browser monitor differ from URL Sequence monitor?

The URL sequence monitor supports only the recording of URL sequences and not the actions performed in the URLs. Also, RBM supports playback from different geographical locations unlike a URL sequence monitor.

See Also

Creating New Monitor - Real Browser Monitor

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 (Record & Playback)

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

Real Browser Monitor: RBM provides live End-User experience measurement. RBM opens up a Microsoft Internet Explorer Browser and monitors a web application just like how a real user sees it. It supports playback from different geographical locations.

Monitored Parameters

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Parameter	Description
Monitor Information	
Health	Specifies the health of the monitor based on its dependencies.
Type	Type of Monitoring
URL address	Specifies the URL being monitored
Match Content	The string that is searched in the resulting html page.
Request Method	The request method sent to the HTTP/ HTTPS URL (Get or Post)
Monitored Parameters	
Availability	The current status of the URL / URL Sequence- whether it is up or down.
Response Time	The response time for accessing an URL or total response time of URL Sequence (takes into account the response time of the individual URLs in the Sequence)
Current Status	Current status of the response time. Click on the icon to know its RCA details.

Parameter	Description
Current Page Size	The current page size of the URL in bytes (only in URL monitoring)
% Change in Page Size	The % change between the current page size and the previous page size. (only in URL monitoring)

See Also

Creating New Monitor - URL Monitors

Oracle E-Business Suite Monitor

Oracle E-Business Suite (Oracle EBS) monitor allows you to monitor the availability and performance of Oracle EBS from a centralized web console.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

Monitor Information

Parameter	Description
Name	Denotes the name of Oracle EBS monitor.
Health	Denotes the health (Clear, Warning, Critical) of the server
Type	Denotes the type you are monitoring.
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the server - available or not available.

Connection Statistics

Parameter	Description
Connections	Specifies the number of connections
Active Connections	Number of connections that are active.

Requests Statistics

Parameter	Description
Active Requests	Number of requests that are active
Completed Requests	Number of completed requests

Response Time

Parameter	Description
Average Response Time	Average Response time of the request
Minimum Response Time	Minimum Response time for the request
Maximum Response Time	Maximum Response time for the request

Process Stats

Parameter	Description
Process Name	Name of the process like BDMSPProcess
Heap Size	Heap memory size of the process

See Also

Creating New Monitor - Oracle EBS Server

SAP Server Monitors

SAP monitor allows you to monitor the availability and performance of SAP environment from a centralized web console. SAP monitor takes advantage of the SAP CCMS (Computer Center Management System) architecture to give insightful information about the SAP system along with fault management and reporting capabilities.

Availability tab, gives the Availability history for the past 24 hours or 30 days. Performance tab gives the Health Status and events for the past 24 hours or 30 days. List view enables you to perform bulk admin configurations.

Monitored Parameters

The following parameters are monitored for SAP. The description for the parameters are from SAP Help - Alert Monitor

Parameter	Description
Monitor Information	
Health	Specifies the health of the monitor based on its dependencies
Type	Type of the Monitor
Host Name	Specifies the host in which SAP is running
Host OS	The Operating System of the host
Last Polled at	The time at which last polling happened
Next Polled at	The time at which the next polling is scheduled
Availability	The current status of the SAP Monitor- whether it is up or down.
Background Processing	
Background Utilization	Percentage of the background processing capacity currently utilized.
System Wide Queue Length	Number of jobs that are ready to be executed, have start authorization, and have no target server specified for which there are no free background work processes, averaged over all application servers with background work processes.
System Wide Free Processes	Number of free background work processes

Parameter	Description
Server Specific Queue Length	Number of released jobs that are explicitly to be executed on this application server, but for which there are no free background work processes
Background work processes count	Number of background work processes on an application server
Error count	Number of errors in background work processes since the monitoring segment was created (that is, since the application server was started)
Error frequency	Number of errors in background work processes per minute
Terminated on error count	Number of background work processes terminated after an error
Buffer	
Hit Ratio	Percentage of the database queries that were met from the buffer (hit rate) and did not have to be passed on to the database for different buffer types like Program, Repository, Table & GUI
Directory Used	Percentage usage of the directory (number of entries) for different buffer types like Program, Repository, Table & GUI
Space Used	Percentage usage of the buffer storage for different buffer types like Program, Repository, Table & GUI
Swap	Swaps due to a full buffer per minute for different buffer types like Program, Repository, Table & GUI
Dialog	
Frontend Response Time	Average time that a user waits at the front end for the processing of his or her request
Database Request Time	Average time for processing logical database requests
Load And Generation Time	Average load and generation time of CUA objects
Response Time	Average response time of the dialog service
Network Time	Time used in the network during the first data transfer from the front end to the application server and during the last data transfer from the application server to the front end.

Parameter	Description
Users Logged In	Number of users logged on
Queue Time	Average time in the dispatcher wait queue
Enqueue	
Enqueue Requests	Number of lock requests
Enqueue Request Rejects	Number of rejected lock requests
Enqueue Requests Errors	Number of errors that occurred during lock requests
Dequeue Requests	Number of release requests
Dequeue Requests Errors	Number of errors that occurred when releasing locks
Dequeue All Requests	Number of releases of all locks of an LUW
CleanUp Requests	Number of releases of all locks of an application server
Backup Requests	Number of update calls for which locks were forwarded to the update.
Reporting Requests	Number of operations for reading the lock table.
Owner Names Actual Utilization	Current number of lock owners in the lock table
Granule Arguments Actual Utilization	Current number of different lock arguments in the lock table
Granule Entries Actual Utilization	Current number of elementary locks in the lock table
Update Queue Actual	Current number of open update requests with locks
Recent Lock Time (per minute)	Time spent in the critical path of the lock table for lock operations (in seconds per minute)
Recent Lock Wait Time (per minute)	Wait time of parallel processes before entering the critical path of the lock table (in seconds per minute)

Parameter	Description
Recent Server Time (per minute)	Total time spent in the enqueue server (in seconds per minute)
Enqueue Frequency	Enqueue operations (logical data locks) per minutes that are coming from another instance to the central instance
Operating System	
CPU Utilization	Average usage of the CPU in a host system
Disk Utilization	Average usage of the disk in a host system
Extended Memory	Utilization of the extended memory as a percentage.
Private Memory	Utilization of the private memory as a percentage.
Roll Area Usage	Usage of the roll area as a percentage
Page In	Average number of page-ins per second; a page-in occurs if a process must access a data page that is not available in the main memory
Page Out	Average number of page-outs per second (page-out occurs if a page is stored out of the main memory to make room for the pages required by other processes)
Syslog Frequency	Number of messages per minute that appeared in the system log of an application server.
Spool system Details	
Spool Utilization	Utilization of the spool work processes as a percentage
Spool Work Processes Count	Number of spool work processes
Spool Work Processes Errors	Number of errors in spool work processes
Spool Work Processes Terminated	Number of spool work processes that terminated after errors
Dispatcher Queue Utilization	Used area of the dispatcher queue as a percentage
Request Queue Utilization	Used area of the spool request queue as a percentage

Parameter	Description
Service Queue Priv	Used area of the spool request queue for processing in chronological order as a percentage
Service Queue Pages	Number of pages in the spool request queue
Device Cache Used	Used area of the entire device cache as a percentage
Device Cache Fixed	Used area of the fixed device cache as a percentage
Host Spool List Used	Used area of the host spool request list as a percentage
Alerts	Shows all the alerts under System Errors tree node of SAP CCMS monitor [RZ 20]. When you set an alert to completed status, it is deleted from the active alerts that are shown in the Alert Monitor and the Alert Browser.

See Also

Creating New Monitor -SAP Monitors

SAP CCMS Monitors

Applications Manager allows you to monitor the availability and connection time of SAP CCMS monitors from a centralized web console. The availability tab, gives the availability history for the past 24 hours or 30 days. The connection time refers to the time taken by Applications Manager to connect to SAP server. You can also add performance / status / log attributes in the same page by clicking on link '**Add Attributes**' or by clicking on '**Add Custom Attributes**' under **Quick Links** section.

Monitored Parameters

The following parameters are monitored for SAP CCMS.

Parameter	Description
Monitor Information	
Health	Specifies the health of the monitor based on its dependencies
Type	Type of the Monitor
Host Name	Specifies the host in which SAP is running
Host OS	The Operating System of the host
Last Polled at	The time at which last polling happened
Next Polled at	The time at which the next polling is scheduled
Availability	The current status of the SAP CCMS Monitor - whether it is up or down.

Adding SAP CCMS Attributes

To add a SAP CCMS monitor set's attributes, follow the steps given below:

1. Click on Add Attributes or Add Custom Attributes link in SAP CCMS monitor page.
2. In the Add Attributes screen, you will find the entire set of CCMS monitoring tree elements (MTE) listed below. Click on MTE which you would like to monitor, and this will expand the entire set of attributes available inside the monitor set.
3. Similarly, you can also select various MTE and its attributes inside available CCMS monitors.
4. If there are no attributes present inside MTE, an error message appears: *"There are no Performance / Status / Log Attributes present in this Node"*

5. Click on Add Attributes button to complete the process.
6. If you would like to delete existing attributes, click on Add Custom Attributes link. In SAP Custom Attributes screen, Applications Manager will list the existing attributes that are being monitored and provides you the option to delete attributes. You can also enable / disable reports for the attributes in the same screen.

See Also

Creating New Monitor -SAP Monitors

Custom Monitors

The following custom monitors are available in Applications Manager.

- JMX / SNMP Dashboard
- File System Monitor
- Windows Performance Counters
- Script Monitors
- Database Query Monitor

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. *Availability* tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. 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

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. For Numeric attributes, you can edit and set whether you want to view the values as Counters or Non Counters. From the next poll onwards, the latest type would be displayed.
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 Alarm 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 alarms 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

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. Click on **Add attributes** link.
2. It opens up Customize screen - Select a **SNMP monitor** from the combo box for adding the attributes. Click add.
3. **Mib Browser** opens up - select the MIB that contains the attribute to be added to the Custom Monitor.
4. Select the **attributes** that you want to monitor. Click **Add** to add the selected attributes.

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 **Add Mib** Form.
- The MIB must be implemented in the SNMP Agent being monitored.

File / Directory Monitor

Applications Manager uses this File / Directory Monitor to monitor the changes in the selected files and directories. *Availability* tab, gives the Availability history for the past 24 hours or 30 days.

Performance tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information.

File Monitor	Checks
File size	the size of the file
File Size changed	the % change in file size
Content	string that needs to be monitored
Last Modified Time	the time at which the file was last modified

Directory Monitor	Checks
Directory Size	the size of the directory
Directory Size changed	the % change in directory size

Important Note:

- File Name / Directory Name should be specified with Absolute Path. (eg) C:\Desktop\test.txt (or) /home/test/test.txt
- In case of Multiple Checks for Content in File Monitoring specify them as comma separated. (eg) NullPointerException,File System Monitor,testString
- Ensure that the file you are monitoring has Read Permission.
- If the file is in Windows server, Content Matching is not supported.
- To access a Shared Folder, the file path should be given like: \\<hostname>\C\$\Vim
- To monitor a Directory in a remote windows server, ensure that the directory has share permissions, thereby making it available locally. Continue to configure the directory in the local server setup.

See Also

Creating New Monitor - File / Directory Monitor

Windows Performance Counters

Applications Manager uses **WMI (Windows Management Instrumentation)** for monitoring Windows Performance Counters. WMI gives preinstalled performance counter classes; each class describes an object in performance libraries.

For eg., the object that appears in the **Perfmon System Monitor** named *NetworkInterface* is represented in WMI by the *Win32_PerfRawData_Tcpip_NetworkInterface* class for raw data *Win32_PerfFormattedData_Tcpip_NetworkInterface* class for pre-calculated, or "cooked" data.

Currently Applications Manager supports monitoring the counters of classes derived from *Win32_PerfFormattedData*

Some of the WMI Performance classes for Performance Objects that are present in Perfmon are

Processor -Win32_PerfFormattedData_PerfOS_Processor

Browser -Win32_PerfFormattedData_PerfNet_Browser

PagingFile -Win32_PerfFormattedData_PerfOS_PagingFile

Memory -Win32_PerfFormattedData_PerfOS_Memory

Server -Win32_PerfFormattedData_PerfNet_Server

Some classes can only have one instance of it, they are called "*Singleton Classes*".

After creating Windows Performance Counters, You will see the *WMI Monitor details* page showing availability and other details. *Availability* tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations. Click on the individual monitors listed, to view the following information. The windows performance counter values can be added and monitored as attributes. The overall ability to configure thresholds on attributes and taking corrective actions are supported out-of-the-box.

Adding Attributes

- Click on *Add Attributes* link.
- This will take you to the list of *WMI Performance Classes*. You can choose the classes whose attributes you want to monitor.
- Click on *Show Attributes*; the list of WMI classes selected along with their attributes and instances are displayed. Select the *attributes* and *instances*. The attributes would then be added for monitoring.
- You can configure thresholds and alarms for the attributes. At a class level, you can configure alarms for Health, which in turn depends on the attributes it comprises of.

Note: Windows Performance Counters is currently supported for **Windows XP, Windows 2000/2003/2008**.

See Also

Creating New Monitor -Windows Performance Counters

Script Monitors

Applications Manager provides Script Monitoring functionality to automatically monitor the output of ad-hoc Windows/Linux/Solaris scripts that are used in-house.

- During creation of a new script monitor, you need to give the **location** of the custom script (local / remote), **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. The output of the script should be in a Key=Value format where '=' can be any delimiter.
- Applications Manager parses the Output File and executes the actions configured. It enables you to alert an Administrator or automatically take corrective actions by way executing other OS scripts.
- Reports for the attributes configured would be shown as graphs. Option to enable or disable reports is given.

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations.

Overriding Availability and Response Time of the Script:

This option would be useful, if you want to override the response time measured for custom scripts using a defined value in the output file. Applications Manager looks for few reserved keywords in the output file, if it matches then it will replace the corresponding attribute.

For eg., if the script output is looking like this,

script_availability=1 (Allowed values are 0 or 1. "0" refers to success. "1" refers to failure.)

script_message=Server is not running.

script_responsetime=10

Then while parsing the output file, script_availability value will be taken and based on that the availability is calculated. The same is the case for response time.

Examples:

Sample Scalar Usecase

Let's assume you want to monitor a script `< filesystem.sh >` present under `/home/test-solaris/` in test-solaris machine. The output from this script is dumped to `output.txt` file present under the same

directory. The format of *output.txt* is as shown below

```
SystemTemperature=37
TimeSinceLastReboot=30
TopPaginApp=sendmail
IOReads=1050
```

Setting up Script Monitor:

- Login to the Applications Manager Web Client.
- Click **New Monitor**. From the combo box, choose **Script Monitor**.
- For the **Display Name** give some name. For e.g FileSystem
- Choose whether the script to be monitored is present in the **Local Server** or in a **Remote Server**. If the script is in a Remote Server, then make sure you put the script in the Remote Server.
- If it is Local Server/ Remote Server, give the absolute path of the Script to Monitor (*/home/test-solaris/filesystem.sh*) and also the absolute path of the directory from which the script should be executed(*/home/test-solaris/*).
- Under Output Settings, give the **Output file name** (*/home/test-solaris/output.txt*) with absolute path. This is the file where the output from the script is dumped.
- Enter the Name of the **Non Numeric** and **Numeric** attributes. In the Numeric area add
<>SystemTemperature
TimeSinceLastReboot
IOReads
Similarly in the String Attributes Textarea add : TopPaginApp
<>
- 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.
- Specify the additional **Arguments** (if required to pass to the script). For e.g., hostname 80
http
- Set the **Polling Interval**. By default, it is 5 minutes
- Specify the **Timeout** value in seconds. The value can be the maximum time taken by the script to execute.
- In Linux, Specify the **mode** in which script should be executed. By default, it is "sh".
- If the script is in a **Remote Server**, select the Host Name from the list
- If the remote server is a new host choose **New Host**, then enter the server's **Host Name / IP Address** (test-solaris). Choose the mode of monitoring - **Telnet** or **SSH**.(Telnet)
- Enter the **User Name**(test) and **Password**(test) of the server.
- Enter the **Port** number - Default Telnet port no: 23, SSH: 22
- Specify the command prompt value, which is the last character in your command prompt. Default value is \$ and possible values are >, #, etc.
- Once all the values are entered select **Add Monitor(s)**.

The success message should be displayed. Click *Monitor Details > Script Monitor* and go to the create script, to view the details.

Sample Table Usecase

Let's assume you want to monitor a script *<prustat.sh>* present under */home/test-solaris/* in test-solaris machine. The output from this script is dumped to *output.txt* file present under the same directory. The format of *output.txt* is as shown below

```
"<--table prustat starts-->"
PID CPU Mem Disk Net COMM
7176 0.88 0.70 0.00 0.00 dtrace
7141 0.00 0.43 0.00 0.00 sshd
7144 0.11 0.24 0.00 0.00 sshd
3 0.34 0.00 0.00 0.00 fsflush
7153 0.03 0.19 0.00 0.00 bash
99 0.00 0.22 0.00 0.00 nscd
7146 0.00 0.19 0.00 0.00 bash
52 0.00 0.17 0.00 0.00 vxconfigd
7175 0.07 0.09 0.00 0.00 sh
98 0.00 0.16 0.00 0.00 kcfid
"<--table prustat ends-->"
```

Note the table headers *<--table prustat starts-->*. This is mandatory and should follow the same format as mentioned. Here "prustat" should be replaced by the Table Name explained below

Setting up Script Monitor

- Follow the same instructions as mentioned for Scalar till point 6
- Select Tables in output file check box
- For the Table Name provide some name(prustat). Note that this same should be present in the table header(*<--table prustat starts-->*) in the output file.
- For the Numeric Attributes area provide the column names in the script output that are numeric
 - CPU*
 - Mem*
 - Disk*
 - Net*
- For the String Attributes provide the column names in the script output that are non numeric
 - PID*
 - COMM*

- For the Unique Column provide the column names that can identify a row data. This can be a single value or multiple value.

PID

COMM

- For the Column Delimiter provide the column separator. The default value is a space.
- In case you have scripts that output multiple tables then you can select More and configure the values.
- Once all the values are entered select Add Monitor(s).

You can use script monitor to monitor the SNMP OIDs

Please look at the steps below for creating a script monitor,

- Create a script file (say script.sh) under the */opt/ManageEngine/AppManager10/* directory
- Edit that file and type in the following content into that file,

```
snmpwalk -v 1 -c public app-w2k1 CPQHLTH-MIB::cpqHeFItTolPowerSupplyRedundant.0.1|
awk '{ y = $1; x = $4 ; gsub(/[/a-zA-Z()]/, "", x)}
{print y " = " x}'>> output.txt
snmpwalk -v 1 -c public app-w2k1 CPQHLTH-MIB::cpqHeFItTolPowerSupplyRedundant.0.2 |
awk '{ y = $1; x = $4 ; gsub(/[/a-zA-Z()]/, "", x)}
{print y " = " x}'>> output.txt
```
- Click on "New Monitor" in applications manager and choose script monitor. Then create a new monitor using the following parameters,

Script to Monitor </opt/ManageEngine/AppManager10/script.sh>

Directory from which the script should be executed </opt/ManageEngine/AppManager10/>

Under Output Settings, Output File </opt/ManageEngine/AppManager10/output.txt>

Numeric Attributes <CPQHLTH-MIB::cpqHeFItTolPowerSupplyRedundant.0.1>

<CPQHLTH-MIB::cpqHeFItTolPowerSupplyRedundant.0.2>

Then use the default parameters for configuring the remaining attributes.

Note: See another simple example of forcing a key value pair into a output file, discussed in our forums.

See Also

Creating New Monitor - Script Monitors

Java Runtime Monitor

Java Runtime Monitor provides out-of-the-box remote monitoring and management on the Java platform and of applications that run on it. It monitors performance metrics like Memory (JVM), Garbage Collection (GC) and Thread Statistics. Thresholds can be associated and alarms generated. Further, operations such as Automated Thread dump ,Heap dump and PerformGC for management are also supported.

The different JVM vendors supported by Applications Manager are Sun JVM, IBM JVM and Oracle JRockit JVM.

Note: Support is available for JRE1.5 and above for Java Runtime. Support for Heap dump operation is available if HotSpotDiagnostic MBean is present in the JVM.

The *Availability* tab gives the Availability history for the past 24 hours or 30 days. The *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. The *List view* enables you to perform bulk admin configurations. Java Runtime Monitor checks the **availability, response time, connection time** (time taken by the Applications Manager to look up the JMX agent on the remote JVM) of the monitor, along with many other parameters listed below.

Parameter	Description
Monitor Information	
Name	Name of the JavaRuntime monitor.
Health	Specifies the health (Clear, Warning, Critical) of the JavaRuntime monitor
Type	Specifies the type you are monitoring.
Host Name	Specifies the host at which the Java virtual machine is running.
Port	Specifies the port number at which the Java virtual machine is running.
Host OS	Specifies the OS of the host where the JavaRuntime monitor is running.
JVM	Specifies the Java virtual machine name and version.
Vendor	Specifies the Java virtual machine Vendor Name.
Processor Count	Specifies the number of processors available to the Java virtual machine.

Parameter	Description
Last Polled at	Specifies the time at which the last poll was performed.
Next Poll at	Specifies the time at which the next poll is scheduled.
Availability	Shows the current status of the JavaRuntime monitor - available or not available.
Connection Time	Time taken to connect to the Java virtual machine.
Memory Pool	
Eden Space (Heap Memory)	The pool from which memory is initially allocated for most objects.
Survivor Space (Heap Memory)	Pool containing objects that have survived GC of eden space.
Tenured Generation (Heap Memory)	Pool containing objects that have existed for some time in the survivor space.
Java Heap	Space where the JVM stores the objects.
Permanent Generation (Non-Heap)	Holds all the reflective data of the virtual machine itself, such as class and method objects. With JVMs that use class data sharing, this generation is divided into read-only and read-write areas.
Code Cache (Non-Heap)	Memory used for compilation and storage of native code.
JIT Code Cache	Memory that is converted to assembler and stored for running at higher speed.
Nursery	Separate space for newly allocated objects.
Thread Parameters	
Total threads started	Total number of threads created and also started since the Java virtual machine started.
Peak Threads	Peak live thread count since the Java virtual machine started or peak was reset.
Live Threads	Number of live threads currently running.
Daemon Threads	Number of daemon threads currently running.
Runnable Threads	A thread executing in the Java virtual machine is in this state.
Blocked Threads	A thread that is blocked waiting for a monitor lock is in this state.

Parameter	Description
Waiting Threads	A thread that is waiting indefinitely for another thread to perform a particular action is in this state.
Timed waiting Threads	A thread that is waiting for another thread to perform an action, for up to a specified waiting time is in this state.
Deadlocked	Number of threads that are in deadlock waiting to acquire object monitors.
Class Loading	
Classes loaded	Number of classes loaded
Classes Unloaded	Number of classes unloaded
JVM Statistics	
CPU Load	Specifies the percentage of load on the machine caused by the JVM. 0 indicates no load is created and 100 indicates all load is created by the JVM.
CPU Usage	This indicates the CPU usage of the JVM on the server.
Max file descriptor	Maximum permissible open file descriptor. Available only for UNIX.
Host Memory	
Total Physical Memory	Total amount of physical memory in Megabytes.
Free Physical Memory	The amount of free physical memory in Megabytes.
Total Swap Space	Total amount of swap space in Megabytes.
Committed Virtual Memory	The amount of virtual memory that is guaranteed to be available to the running process in Megabytes.
Garbage Collector	
Time Spent/Min	Approximate collection elapsed time in milliseconds.
Collections/Min	Total number of collections that have occurred.
Thread Count	Number of threads used for Garbage Collector.
Last Start Time	Start time of this GC.
Last End Time	End time of this GC.

Parameter	Description
Memory usage before GC	Memory usage of all memory pools at the beginning of this GC.
Memory usage after GC	Memory usage of all memory pools at the end of this GC.
GC time	Time taken to perform garbage collection.
Compile time	Time spent in just-in-time (JIT) compilation.
Configuration	
Uptime	The uptime of the Java virtual machine.
Java Virtual Machine	The Java virtual machine implementation name.
Vendor	The Java virtual machine implementation vendor.
Process ID	The process identifier is a number used by some operating system kernels to uniquely identify a process.
Name	The name representing the running Java virtual machine.
VM arguments	The input arguments passed to the Java virtual machine which does not include the arguments to the main method.
Class path	The Java class path that is used by the system class loader to search for class files.
Library path	The Java library path.
Boot class path	The boot class path that is used by the bootstrap class loader to search for class files.
JIT compiler	The name of the Just-in-time (JIT) compiler
Objects Pending for finalization	The approximate number of objects for which finalization is pending.
Operating System	The name of the operating system.
Architecture	The operating system architecture.
Processors	The number of processors available to the Java virtual machine.

The table below lists the different JVM vendors supported by Applications Manager and the major parameters monitored by them.

Parameters Monitored	Sun JVM	IBM JVM	JRockit JVM
Connection Time	✓	✓	✓
Memory Usage	✓	✓	✓
CPU Usage	✓	✓	
CPU Load			✓
System Memory	✓	✓	✓
Process Memory	✓	✓	✓
Heap Memory	✓	✓	✓
Non Heap Memory	✓	✓	✓
VM Statistics	✓	✓	✓
Total Physical Memory	✓	✓	
Free Physical Memory	✓	✓	
Total Swap Space	✓		
Free Swap Space	✓		
Committed Virtual Memory	✓		
Garbage Collector- Summary	✓	✓	✓
Garbage Collector - View impact for specific collector	✓		
Total Threads Started	✓	✓	✓
Peak Threads	✓	✓	✓
Live Threads	✓	✓	✓
Runnable Threads	✓	✓	✓
Blocked Threads	✓	✓	✓
Waiting Threads	✓	✓	✓
Timed Waiting Threads	✓	✓	✓
Daemon Threads	✓	✓	✓
Deadlocked	✓	✓	✓
Configuration Details	✓	✓	✓
JVM Actions	✓	✓	✓

View Thread Dump

There is an option to view the thread dump history under 'Threads' tab. Click the 'View Thread Dump' link in the threads tab. The *Thread Dump* screen will open up in a new window and you will be able to view the current thread dump details. Once you close this window, the thread dump details will be moved under the *Thread History* section. You can view this information any time you want from this section.

Reports

We provide the option to view both realtime and historical data of any of the attributes present in the 'Configuration Information' section in the *Configuration* tab. Click on any attribute under the Configuration tab. This will open up a new window named 'History Data' that provides more information about these attributes.

There are two tabs in the *History Data* window - History Report and Global View

History Report: This tab provides historical reports of the attribute selected based on time period chosen. You can also use the *Select Attribute* drop-down box and view reports for other attributes.

Global View: This tab displays the current values of the attribute selected, across multiple monitors. To view information about other attributes present in the monitor, use the *Select Attribute* drop-down box and change the attribute.

If you want to view data of multiple attributes, click the *Customize Columns* link present at the top left corner of the window. This will take you to the *Edit Global View* screen. In this screen, you can change the monitor type using the *Filter by Monitor Type* drop-down box, select the metrics to be displayed, and show monitors on a monitor basis or a monitor group basis. After you select your options, click the *Show Report* button to view those information in the *Global View* tab.

Few Help Links for Reference:

Tuning Garbage Collection with the JVM

FAQ About the Java HotSpot VM

FAQ about Garbage Collection in the Hotspot JVM

Java Performance Documentation

See Also

Creating New Monitor - Java Runtime Monitor

Database Query Monitor

Database Query Monitor is used to monitor a single or a specific set of queries for any given database.

- *Availability* tab, gives the Availability history for the past 24 hours or 30 days.
- *Performance* tab gives the Health Status and events for the past 24 hours or 30 days.
- *List view* enables you to perform bulk admin configurations.

Using a single query or a given set of queries, you can monitor the status of any given database using Applications Manager Database Query monitor. Queries are the best way to find out whether your database is up and running 24x7. In business enterprises such as an online store, there are a number of applications and databases used for e-commerce. Any interruption in such an environment could mean only one thing: loss of revenue.

The execution of such a query or a set of queries can be automated by setting the polling interval. By fixing the polling interval, user can automate this process and the results are obtained at the end of the polling. The result includes execution time (time taken by the query to provide results) and also displays any error that may occur during regular polling intervals. These errors help identify any issue that may occur with the database.

Let us consider an example. Many enterprise environment run critical applications which need to be up and running 24x7. Let us assume, the status of such applications are maintained in a "APPLICATIONS_STATUS" table. Using Database Query monitor, the user shall be able to send a select set of queries to that database to find out if they are operational or not.

APPLICATIONS_STATUS		

APPLICATIONS_NAME	Status	

PURCHASE	OK	
CRM	CRITICAL	
PAYROLL	OK	
LEADS	OK	

SELECT * APPLICATIONS_STATUS

By executing the above command using Database Query monitor, the user will then obtain the list of applications that are running along with its status. The user can then identify the applications whose

status is '**Critical**' and then carry out necessary action by configuring Alarms in Applications Manager. This action could be in the form of creating a ticket, or executing a script to rectify the problem.

Database Query monitor can also be used to identify any bottle necks in the networks which are linked to several databases and help remove them by identifying the correct database which has the issue. This bottle neck issue can arise because there is a problem with the one of applications or with the databases. Using Database Query monitor, user can then execute a given set of queries and analyze the result which provides a clear indication of the error that has caused such an occurrence. The result includes the execution time (time taken by the query to generate the result). If the execution time is above a certain pre-assigned threshold, then the issue is with the database or if the result is below the pre-assigned threshold, then the issue is elsewhere.

The Database Query monitor currently supports the following set of databases queries:

- MySQL
- MS SQL
- Sybase
- DB2
- Oracle and
- Postgres

Applications Manager also provides the ability to compare various column value in the output by attributes types. Option to Enable or Disable Reports is provided.

Note: Please note that the number of queries is limited to five queries. Total number of rows shown in the output is limited to 50 rows.
--

J2EE Web Transaction Monitors

J2EE Web Transaction Monitors

J2EE 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.

J2EE Web Transaction Monitor requires an **agent** to be plugged in the server to be monitored. Know more about J2EE Web Transaction Agent.

Through the agent, the **performance metrics** data is collected for the URLs invoked by the server and is displayed in the J2EE web transaction monitor. Know more about Performance Metrics

Availability tab, gives the Availability history for the past 24 hours or 30 days. *Performance* tab gives the Health Status and events for the past 24 hours or 30 days. *List view* enables you to perform bulk admin configurations.

See Also

Creating New Monitor - J2EE Web Transactions Monitor

J2EE Web Transaction Agent

J2EE 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 **WebTransactionAgent.jar** present under `<ApplicationsManagerHome>/working/resources` 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 WebTransactionAgent.jar>`
- Restart the Application server (*like JBoss, Tomcat*).

For e.g., To enable J2EE Web Transaction Monitor in JBoss application Server, do the following :

- Copy the J2EE web transactions agent(*WebTransactionAgent.jar*) under `<ApplicationsManagerHome>/working/resources` 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 WebTransactionAgent.jar>`
- Restart JBoss.

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.

J2EE Web Transaction Agent Configuration

Configuration is driven via the **wta.props** file. Properties in wta.props are

- **port** - port in which Agent wil start. The default port of the agent is 55555. You can change the default value to your requirement.
- **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 speccied as *exclude* then all the packages except for the ones mentioned in the package-list are selected for instrumentation.
- **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>`).

To configure the wta.props file in your Application Server, add `-Dam.wtaconf.dir=<directory in which the wta.props file is present>` in JAVA_OPTS . A sample wta.props file is present under `<AppManager10/working/conf>`

To verify if the agent has started, look for the message '*J2EE Web Transaction agent started at port*

|<55555>' in the startup logs.

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 - J2EE Web Transactions Monitor

J2EE 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.

Alarm Configuration:

By clicking on the **Configure Alarm** icon, you would be able to configure alarms 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 alarm configuration. Action can be configured at the monitor level for the Health and Availability. The alarms 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 - J2EE Web Transactions Monitor

ManageEngine OpManager Network Monitoring Connector

ManageEngine Applications Manager integrates now with a comprehensive Network Monitoring Tool, ManageEngine OpManager. ManageEngine OpManager provides an effective network monitoring software that offers comprehensive fault and performance management across WAN and all other IT infrastructure. Using Network Monitoring Connector, an Applications Manager User can view the status of his Network Devices in addition to Servers, Application Servers, Databases monitored by Applications Manager.

Key Benefits:

1. Single console to monitor Network, Server & Applications.
2. View SLA and Availability Metrics of your Business Application by taking in to consideration the network, servers and applications.
3. Single console to view all Alarms.

To Configure OpManager:

In order to collect data, you need to configure OpManager properly.

1. Login into OpManager.
2. Proceed to **Admin** tab and click on **User Manager**. Under User Manager, you will find **Add User** option.
3. Click on **Add User** with user permission as **Read Only Access**.

To Configure Applications Manager:

Once OpManager is configured correctly, now you need to configure Applications Manager to obtain the data from OpManager.


1. Login into Applications Manager.
2. Click on the **Admin** tab in Applications Manager.
3. Click to **Add-on/Product Settings**.
4. Enter the **Server name** and **Port number** of the machine where OpManager is running. Enter the **Username** and **Password** of the Read Only user created in OpManager.
5. Click **Save** button to save the settings.

Associate network device Monitors into existing Monitor Groups:

1. In order to associate OpManager monitor against a Monitor Group in Applications Manager, click on the **Home** tab.

2. Under **Monitor Group Information**, click **Associate Monitor** of Monitor Group Links in the left frame.
3. A list of discovered Monitors (for both Applications Manager and OpManager) that are available for associating and those that have already been associated with that Monitor Group is displayed. You will also see a list of network devices under **Network Devices** being displayed.
4. Select the check box of the corresponding Monitor from **Monitors not present in this Monitor Group** list and click **Associate**. 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**.
5. Click on **Monitors** tab to view the list of network devices that are now configured. Clicking on **Network Devices** in category view would provide the availability and performance of all the Monitors associated under it. For example, if you have configured a server to be monitored, the performance metrics that are shown in Applications Manager are: availability, response time, CPU, Memory and Disk utilization and so on.

Associate network device Monitors into a new Monitor Groups:

1. Click on the **New Monitor Group**.
2. Provide a Monitor Group name, description of that monitor group and assign the owner for the monitor group.
3. Once the Monitor Group is created, click on **Associate Monitors** provided in the **Summary** tab of that Monitor Group.
4. A list of discovered Monitors (both Applications Manager and OpManager) that are available for associating is displayed. You will also see a list of network devices under **Network Devices** being displayed.
5. Select the check box of the corresponding Monitor from the list and click **Associate**.
6. Click on **Back to Monitor Group** to view the list of Monitors that you have associated for that group. 

ManageEngine OpStor SAN Monitoring Connector

ManageEngine Applications Manager integrates with the comprehensive Storage Monitoring Tool, ManageEngine OpStor. OpStor is a heterogeneous storage infrastructure monitoring solution that helps enterprises to monitor their storage resources. Using OpStor SAN Monitoring Connector, an Applications Manager User can view the status of his Storage Devices in addition to Servers, Application Servers, Databases monitored by Applications Manager.

Key Benefits:

1. Single console to monitor Storage devices, Server & Applications.
2. Single console to view all Alarms.

To Configure OpStor:

1. Login into OpStor.
2. Proceed to **Admin** tab and click on **User Manager**. Under User Manager, you will find **Add User** option.
3. Click on **Add User** with user permission as **Read Only Access**.

To Configure Applications Manager:

Once OpStor is configured correctly, you need to configure Applications Manager to obtain the data from OpStor

1. Login into Applications Manager.
2. Click on the **Admin** tab in Applications Manager.
3. Click to **Add-on/Product Settings**.
4. Click on **OpStor- Add** link. Enter the **Server name** and **Port number** of the machine where OpStor is running. Enter the **Username** and **Password** of the Read Only user created in OpStor
5. Click **Save** button to save the settings.

Associate network device Monitors into existing Monitor Groups:

1. In order to associate OpStor monitor against a Monitor Group in Applications Manager, click on the **Home** tab.
2. Under **Monitor Group Information**, click **Associate Monitor** of Monitor Group Links in the left frame.
3. A list of discovered Monitors (for both Applications Manager and OpStor) that are available for associating and those that have already been associated with that Monitor Group is displayed. You will also see a list of network devices under **Network Devices** being displayed.

4. Select the check box of the corresponding Monitor from **Monitors not present in this Monitor Group** list and click **Associate**. 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**.
5. Click on **Monitors** tab to view the list of network devices that are now configured. Clicking on **Network Devices** in category view would provide the availability and performance of all the Monitors associated under it. For example, if you have configured a server to be monitored, the performance metrics that are shown in Applications Manager are: availability, response time, CPU, Memory and Disk utilization and so on.

Associate network device Monitors into a new Monitor Groups:

1. Click on the **New Monitor Group**.
2. Provide a Monitor Group name, description of that monitor group and assign the owner for the monitor group.
3. Once the Monitor Group is created, click on **Associate Monitors** provided in the **Summary** tab of that Monitor Group.
4. A list of discovered Monitors (both Applications Manager and OpStor) that are available for associating is displayed. You will also see a list of network devices under **Network Devices** being displayed.
5. Select the check box of the corresponding Monitor from the list and click **Associate**.
6. Click on **Back to Monitor Group** to view the list of Monitors that you have associated for that group.

Alarms



What is an Alarm?

Alarms 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 Alarms and they are

- Critical > 
- Warning >  and
- Clear > 

Alarms 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. Alarms 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.
- Alarms are also generated based on dependencies configured to the attributes. Refer to Configuring Dependencies section for more details.

The Alarms screen provides the following:

- **Alarms Graph:** This graphically represents the number of alarms based on its severity.
- **Alarm Views:** This is an option to view the alarms based on a particular Monitor Group or Monitor Type by selecting them from the respective combo box.
- **Alarms list:** This lists all the alarms with details such as Monitor name, Status, Alarm Message, Date/Time, and Technician who attended on the Alarm. You have an option to display 25/50/75/100/125 Alarms per page. Alarms can be acknowledged by the Technicians (Users) by picking up alarms, likewise unpicking of alarms 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 alarms from Critical/Warning to Clear state. By clicking on the 'Alarm Message' link, you can view the Alarm Details. Also, you can view the history of the alarm by clicking on the **History Report** PDF.
- **Alarms for traps:** Traps received via SNMP Trap Listener can be seen here. Also, the other unsolicited traps can be viewed here.

- **JMX Notifications:** You can view the JMX Notifications received.
- **Quick Links:** Refer to the Alarm Details section.

The following steps will generate alarms 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 Consecutive Polls

Note: Bulk Alarms Configuration is also possible. Refer Bulk Alarm Configuration

Alarm Details

Under Alarms tab, By clicking on the 'Alarm Message' for individual alarms, the alarm details for each alarm is displayed.

Alarm Details Page:

Under the Alarm Details page, you can view the time at which the alarm was created, Severity, Previous Severity of the alarm and Root Cause Analysis. Further, annotations can be made to explain the details of the alarm. Then, you have the **Alarm History** displayed. Alarm history gives you the history of the changes in the status of alarm over a period of one week.

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 Alarms page.

All	Lists all the alarms based on Alarm Views where there are options to choose a particular or all Monitor Groups and Monitor Types.
Last One Hour	Lists all the alarms generated for the last one hour.
Last One Day	Lists all the alarms generated for the last one day.

Recent 5 Alarms

Under Home tab, the recent 5 alarms generated (critical and warning) is listed with 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 alarm.
- **Message:** Refers to the problem that caused the alarm. Click on the message to know more about the alarm details. Also view the Alarm History that gives you a detailed idea on generation of the alarm and its status.
- **Time:** Time at which the alarm is generated.

Alarms Summary

Lists the recent critical alarms of Applications Manager. You can view the alarm summary by clicking in the graph icon near the printer friendly icon.

Note: Also, check out the blog post about RCA Messages.

Viewing and Configuring Alarms Globally

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

Once the Monitor is associated with the Monitor Group, alarms can be configured through the **Configure Alarm** 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.

How to Demos: Have a look at our demo on configuring Alarms in our website.

The purpose of Global Alarm 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 alarms' page, herein you can create a new threshold or apply an existing threshold for the attribute.

Note: By selecting 'Apply to selected monitors', the threshold for this attribute is applied to selected / 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 selected monitors', the threshold for response time can be applied to all Linux servers or to a select number of 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 Alarm Configuration screen by clicking 'Configure Alarms' 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 alarms. You can also specify a message that has to be appended to the alarm. 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 Consecutive 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 Alarm Configuration instead of the individual Monitor screen.

Refer to Associating Threshold and Action with Attributes for more details. [View Related Blog](#)

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 alarms 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:

Note: Have a look at Creating actions - How to Demos in website.



- Sending E-mail
- Sending SMS
- Executing Program
- Sending Trap
- Execute MBean Operation
- Log a Ticket
- Perform Java Action
- Amazon EC2 Instance Action
- Virtual Machine Action
- Replaceable Tags

Sending E-mail

This action will send e-mail to the specified persons in the event of an alarm. 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 see 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 alarm information generated by Applications Manager to the Email.
 6. If you want to execute the action during specific time periods, enable the **Execute Action during Selected Hours** option and select the Business Hour during which the action has to be executed.
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. Further, you can edit the EMail template by changing `<mail.html>` file present in the `<AppManager10>/working/conf` directory. Restart Applications Manager on changing `<mail.html>`.



Sending SMS

This action can be used to send SMS (Short Message Service) to specific users in the event of the alarm. 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. Choose the mode of SMS - Either through EMail or through Modem.
 3. In case of EMail, enter the **from** and **to** addresses.
 4. In case of Modem [Available in Windows only], enter the **mobile number** to which the message has to be sent. You should have configured the SMS Server beforehand to use this facility. To know more about sending SMS through modem, refer Admin - Configure SMS Server.
 5. 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-Alarm-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 alarm, a specific program can be executed. To execute a program, follow these steps:



Note: Windows Server is not supported

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. Choose whether the program to be executed is from the local server or from a remote server.
 3. If the program is in a remote server, choose the Host Name from the list of existing servers or else you can add a new host.
 4. For configuring a new host, enter the following details - Host Name / IP Address, Mode of monitoring (Telnet/SSH), User Name and Password of the host, port number (Default Telnet port no: 23, SSH port no: 22) and then specify the command prompt value, which is the last character in your command prompt. Default value is \$ and possible values are >, #, etc
 5. Enter the Program to be executed. Use the Upload Files/Binaries option to upload the script file .
 6. Enter the directory path from which the script should be executed.
 7. 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 alarm processing is held up by the program execution. That is, while executing the program, the command runs synchronously in the mail alarm processing thread. This will delay all the alarms, following the

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.

Usages : Pointers to where you can use Execute Program action

- Integrate a .vbs script to be executed by writing a simple .bat file. With this you can restart a remote service, reboot a machine etc.
- Execute custom actions like calling a python script or Java class etc.
- Invoke a .wav file to make some alarm noise on the server
- Execute a script on a remote server
- Trigger actions like cleaning up a harddisk when the usage exceeds some threshold limit

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 alarms 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 alarm 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.

Note: You can configure alarm actions (for eg., EMails to be sent) for unsolicited traps. Refer FAQ.

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 loginLevel 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 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 alarm. 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 alarm message that was generated, to the trouble ticket.

Note: More information on how to integrate ServiceDesk Plus with Applications Manager is available [here](#)

Perform Java Action

This action will perform Java actions such as generating thread dump, heap dump or garbage collection in the event of an alarm. To create a Java action, follow the steps given below:

1. Select the **Java Heap Dump/Thread Dump/GC** option from the **Actions** menu.
2. Enter the **Display Name** of the action.
3. Choose the **Action Type** to be performed in the event of an alarm. You can choose either 'Thread Dump', 'Heap Dump' or 'Perform GC' option.
 1. If you choose the 'Thread Dump' option, specify the **Number of thread dumps** to be performed and the **Delay between thread dumps** in seconds.
 2. If you choose the 'Heap Dump' option, specify the **Number of heap dumps** to be performed and the **Delay between heap dumps** in seconds.
 3. If you choose the 'Perform GC' option, specify the **Number of GCs** to be performed and the **Delay between GCs** in seconds.
4. Select the email action to be associated with this Java action using **Associate Email Action**. You can either select an existing email action from the drop-down box or create a new email action by clicking the 'New Action' link.
5. **Select Target JRE** for this action from the drop-down box. The available options include Auto-select JRE, All JREs in the selected monitor group, Specific host and Specific JRE.
 1. If you select **Auto-select JRE**, Applications Manager will automatically detect and trigger Java actions based on the associated monitor. For example, if the action is associated with a host, this will trigger thread dump for the JREs available in the host. Or if the action is associated with a Tomcat/JRE monitor, this will trigger thread dump for the JREs present in the host of Tomcat server or JRE.
 2. If you select **All JREs in the selected monitor group**, this will trigger java actions for all the JREs present in that monitor group.
 3. If you select **Specific host** option, this will trigger java actions for all the JREs present in the selected host.
 4. Selecting a **Specific JRE** will trigger java actions for that JRE.
6. Click the **Create Action** button to finish creating the Java action.


After creating the Java action, you can test its execution by clicking the **Execute** icon  of that action.

Perform Amazon EC2 Instance Action

This action can be used to start/stop/restart Amazon EC2 instances in the event of an alarm.

To create an Amazon EC2 instance action, follow the steps given below:

1. Select the **Amazon EC2 Instance Action** option from the **Actions** menu.
2. Enter the **Display Name** of the action.
3. Choose the **Action Type** to be performed in the event of an alarm. You can choose either *Start Instances*, *Stop Instances* or *Restart Instances* option.
4. Use the **Select Target EC2 Instance** option to associate the action to EC2 instance(s). There are two ways of selecting the target instance(s).
 1. *All EC2 Instances in the selected monitor group*: This triggers the action for all the instances present in the selected monitor group.
 2. *Specific EC2 Instance*: This triggers the action for the selected EC2 instance alone.
5. You can use the **Notify after action executes** option to receive an email notification once the action is successfully executed. You can either select an existing email address or define new email addresses using the *New Action* option.
6. Click the **Create Action** button to finish creating the Amazon EC2 Instance action.


After creating the Amazon EC2 Instance action, you can test its execution by clicking the **Execute** icon  of that action.

Perform Virtual Machine Action

This action can be used to start/stop/restart virtual machines of VMware ESX and/or Hyper-V servers in the event of an alarm.

To create a virtual machine action, follow the steps given below:

1. Select the **Virtual Machine Action** option from the **Actions** menu.
2. Enter the **Display Name** of the action.
3. Choose the **Host Type** on which the action has to be performed in the event of an alarm. You can choose either *VMware* or *Hyper-V*.
4. Choose the **Action Type** to be performed in the event of an alarm. You can choose either *Start VM*, *Stop VM* or *Restart VM* options.
5. Use the **Select Target Virtual Machine** option to associate the action to a virtual machine. There are three ways of selecting the target virtual machine(s).
 1. *All VMs in the selected monitor group*: This triggers the action for all the virtual machines present in the selected monitor group.
 2. *All VMs in the selected ESX/Hyper-V host*: This triggers the action for all the virtual machines present in the selected ESX/Hyper-V host.
 3. *Specific Virtual Machine*: This triggers the action for the selected virtual machine alone.
6. Specify the **Maximum time for action execution** in seconds. This is the time limit within which the action has to be executed or else the action will be cancelled.
7. You can use the **Notify after action executes** option to receive an email notification once the action is successfully executed. You can either select an existing email address or define new email addresses using the *New Action* option.
8. Click the **Create Action** button to finish creating the Virtual Machine action.


After creating the Virtual Machine action, you can test its execution by clicking the **Execute** icon  of that action.

Windows Services Action

This action can be used to start/stop/restart Windows services in the event of an alarm.

To create a Windows Services action, follow the steps given below:

1. Select the **Windows Services Action** option from the **Actions** menu.
2. Enter the **Display Name** of the action.
3. Choose the **Action Type** to be performed in the event of an alarm. You can choose either *Start Services*, *Stop Services* or *Restart Services* options.
4. Use the **Select Windows Services** option to add windows services. Click the *Add Services* link. The *Add Windows Services* window will pop up. From this window, you can select Windows services using any of the methods described below:
 1. **Select from Windows Servers:** The Windows servers configured in your Applications Manager will be listed in the screen. Select the monitor type and the monitor from the respective drop-down boxes, and click Show Service link. This will list all the Windows services along with their current statuses. You can choose the services you want to add from this list.
 2. **Select from Windows Services Template:** If you select this option, the services associated with the Windows services templates configured in Applications Manager will be displayed on screen. Select the necessary services from this list and click the *Add Services* button to add the services.
5. Specify the **Target Servers** on which these actions are to be executed. There are three options available here:
 1. **Auto-select Servers:** This option will automatically detect and trigger Windows Services action based on the associated monitor. For example, if the action is associated with a host, the action will be triggered for that particular host. If the action is associated with a Tomcat monitor, this action will be triggered for the host of the Tomcat server.
 2. **Selected Servers:** This option lets you specify the exact servers on which the action will be triggered. You can select the servers from the ones listed.
 3. **All Servers in the Selected Monitor Group:** This option lets you specify the exact servers on which the action will be triggered. You can select the servers from the ones listed.
6. You can use the **Notify after action executes** option to receive an email notification once the action is successfully executed. You can either select an existing email address or define new email addresses using the *New Action* option.
7. Click the **Create Action** button to finish creating the Windows Services action.

After creating the Virtual Machine action, you can test its execution by clicking the **Execute** icon  of that action.

Replaceable Tags

Alarm 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 "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.

Tags	Values
\$MONITORNAME	Name of the Monitor
\$MONITORGROUP	Name of the monitor group
\$ATTRIBUTE	Various Attributes like Health, Availability, etc.,
\$SEVERITYASNUMBER	1 (Critical/Down) 4 (Warning) 5 (Clear/Up)
\$SEVERITY	Critical, Warning, Clear, Up and Down
\$HOSTIP	The IP Address of the Host
\$MONITORTYPE	Various Monitor Types like Tomcat-server, MYSQL-DB-server, Script Monitor, etc.,

Tags	Values
\$OBJECTNAME	MBean Object name when associated to Custom Monitor attributes
\$HOSTNAME	Name of the Host
\$PORT	Port Number
\$DATE	Date
\$OID	SNMP OID
\$RCAMESSAGE	Root Cause Message like Average Response Time of SQS_Tomcat-server_9095 is critical because its value 652 > 10ms. [Threshold Details : Critical if value > 10, Warning if value = 10, Clear if value < 10]

Limitation of Dollar tags

\$ATTRIBUTE \$DATE \$MONITORNAME \$MONITORGROUP \$MONITORTYPE \$RCAMESSAGE \$SEVERITY \$SEVERITYASNUMBER	These attributes will work for all the monitors / monitor groups
\$HOSTIP \$HOSTNAME \$PORT	These attributes will not work for Monitor groups / URL / URL sequence monitor / Script Monitor / WMI counters / Web Services.
\$OBJECTNAME	This will work only for JMX custom attributes
\$OID	This will work only for SNMP custom attributes
\$HOSTIP, \$HOSTNAME	These will not work for Ping monitor and File Monitor.

Note: The \$ tags will not be replaced when you execute the actions manually.

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 alarms. Follow the steps given below to associate a threshold and actions with an attribute:

Note: Have a look at Associating Threshold & Action with attributes - How to Demos in website.

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 Alarm** 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 selected monitors' , the threshold for this attribute is applied to the selected monitors.

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 Alarm Configuration screen.

The threshold and/ or actions are now associated with the attribute. Based on this, alarms 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 alarms.

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 alarms.

See Also

Anomaly Profiles

Alarm Escalation

Using this option, you can escalate if any alarm has not been attended to for a given time period. You can configure rules to send Escalation EMail about unattended alarms to the Admin or to the superior.

Alarm Escalation Configuration:

- Under the Admin Tab, Click on Alarm Escalation icon.
- Set the rule. For eg., Send Escalation EMail if the critical alarms of all monitors are not cleared within 2 hours. You can set rules for alarms in individual monitor groups too.
- Give the EMail ID to which Escalation EMail should be sent.
- Set the time period for which the rule should be executed repeatedly.
- [By choosing](#) not to receive duplicate escalation EMail for the same alarm, you opt for optimizing the number of escalation EMail sent. For eg., If there are five critical alarms that were escalated in the first execution run (say 10 minutes), only if there is an addition of new alarm or deletion of alarm, the next set of alarms will be escalated in the second run. If there is no change in the environment in the next 10 minutes, ie., if the five critical alarms still remain the same, escalation EMail will not be sent.

Bulk Alarm Configuration

After configuring alarm for a particular monitor, if the same configuration holds good for all other monitors of the same type, then by using **Alarm Template** functionality you can do Bulk Alarm 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 alarm (Threshold and Action) is configured for one Tomcat server and by using Alarm Template this configuration can be applied to all the other Tomcat servers.

Usage of Alarm Template is illustrated below:

1. Click on the **Alarm 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. Under the Advanced option, you can choose the monitors to which alarm template can be applied.
6. On clicking on **Apply**, the alarm configuration is applied across all monitors of the same Monitor Type.

Configuring Dependencies and Alarm Rules

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

Alarm Rules: They determine the **health/availability** of a Monitors Groups. More

Dependent Devices: You can configure a dependent device in such a manner that if the availability of the dependent device is down, all the Monitors/Monitor Group's availability under the dependent device will be down. Also, you have the option of suppressing all the alarms caused by the dependent device.


Configuring Dependencies for Monitors:

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.

To configure dependencies for the Monitor, 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 Alarm** icon  of the respective Monitor. This opens the Configure Alarm 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 / Alarm 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 Alarm Rules for Monitor Groups:

By configuring Alarm Rules, you can specify how the health or availability depends on the constituent Monitors in that Monitor Group. For eg., using Alarm Rules, you can say Health of the Monitor Group is Critical if the health of any two monitors in the monitor group is critical or Availability of the Monitor Group is Critical if health of any one of the monitors is critical.

To configure alarm rules for the Monitor Group, do the following steps:

1. Select the **Home** tab that lists all the Monitor Groups.
2. Click on the **Monitor Group** you want to configure alarm rules.
3. Click on the **Configure Alarm** icon  of the Monitor Group [under Today's Availability]. This opens the Configure Alarm screen.
4. Select the status you wish to alarm on. Choose **Health** or **Availability** from the combo box.
5. For Availability Alarm Rule, set the rule as -
Monitor Group is down if any/all/selected Monitor's availability is down
or
Monitor Group is down if Monitor's health is critical/warning
6. For Health Alarm Rule, set the rule as -
Monitor Group is Critical if any/all/selected Monitor's availability is down or if Monitor's health is critical/warning
Monitor Group is Warning if any/all/selected Monitor's availability is down or if Monitor's health is critical/warning
7. You have the option of setting any number of rules. For eg., it can be Monitor Group's Availability is down if any one of the monitor's availability is down or if the health of any one of the monitor is critical. Likewise, you can have your customized set of Alarm Rules.

Note: In Alarm Rules

1. Rule processing order will be Down,Critical and Warning i.e., Applications Manager will first process Down rules followed by Critical and Warning.
2. Processing rules will be stopped at any condition if rules is matched, further it won't proceed to process rules.
3. In 'Selected' rule type, Monitor Group status will depend on all the selected monitors severity.

Configuring Dependent Device

To configure dependent device for the Monitor Group, do the following steps:

1. Select the **Alarms** tab. It opens up the Alarm dashboard.
2. Click on the **Configure Alarms** link, found under the list of monitors with critical alerts. It opens up the Global alarm configuration page.
3. Select the **monitor or monitor group** for which you want to configure dependent device
4. Under Availability, click on **Configure Availability**. Then select **Dependent Device** tab. It opens up the Configure Dependent Device screen.
5. From the list of monitors, select the monitor you wish to assign as Dependent Device.
6. You also have the option of suppressing the alarms generated from the Dependent Device.

Note:

1. Sub Group will override MG Group Dependent Device Configuration
2. Monitor level configuration will override all the Dependent Group(Monitor Group and Sub Group) level Dependency configuration
3. Configuring Dependent device at monitor group level is like configuring dependent device for each device under monitor group.

Configuring Consecutive Polls

If you do not want Applications Manager to generate alarm 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 alarm. For e.g., If you want an email alarm 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 Action / Alarm Settings , you can have a common setting for all the monitors.

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 Polls on **Availability** for Individual monitors

1. Click on Configure Alarm 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 Alarm Link in the Snapshot view of the monitor, and by clicking on the Configure Alarm icon, for availability attribute, you can configure the consecutive polls.
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 action / alarm settings for consecutive polls take effect.

To Configure 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 action / alarm 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 alarm 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 action / alarm settings for consecutive polls 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. These calculated predictions allows you to plan for any future impact on performance for various services. To view these 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 dynamically 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. By default, the graph for the attribute reports will be depicted for top 10 monitors.


The reports generated by Applications Manager depicts the availability, health, response time and alarms of the application over a specified period of time. The reporting function enables you to analyze your servers / applications / databases/ web servers / web applications / services even across months and all this even without having to make any additional configuration changes. The reports are generated dynamically, which means that you only see reports for monitors that you have created in Applications Manager. Before proceeding, please ensure that you have enabled reports for all the monitors. The generated reports has 7 / 30 report details which enables you to understand the behaviour of your applications under various business hours or during a particular period of the week/month. This feature allows you to make predictive calculations on future impact.

Some of the common functionalities of reports are as follows:

- Options to view 10/20/50/All reports by choosing them from the **Top N Reports** field. They are enabled by default for all availability and health reports.

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

- Options to schedule reports or enable reports can be done quickly by clicking on '**Schedule Reports | Enable Reports**' link.
- 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. Additionally, you have the option to set the **Business Hours** during which you want the reports.
- Option to view **Custom Attribute Reports** and **Downtime Summary Report** configuration. Click here for detailed information.
- Option to save the reports in **CSV format by clicking on  icon** , **PDF format by clicking on  icon and also save in Excel format** (available only for Monitor Group - Availability & Health Snapshot - Current Snapshot, Critical Snapshot, History report, Outage Comparison Report, Availability Trend Report) for each individual report under reports tab. And also, you can mail these particular report to yourself by clicking on  icon, fill out the email address and click **Send**.

- Option to **delete known Down Time reports**. You can delete known downtime reports from the database by clicking the  icon in the Availability Report. For eg, go to *Application Server* and select *Weblogic* from the pull down menu in the top. Now click on *Availability of Application Servers*. Now click on the monitor's *Total Downtime*. Select the known downtime from the **Monitor Downtime detail***. This will delete this known downtime report from the database.
- **Downtime History**: Gives the downtime/uptime chart for 'today's period and also the downtime history for that particular monitor across all time periods. You can also assign Groups as well as Sub-Groups to downtime scheduler and generate reports. In Downtime history report, you can view the summary details of Scheduled Downtimes and Unmanaged time. This will give you more clarity in knowing the monitor's exact downtime. You can also add notes on why the monitor was down for that particular time period.
- **Summary Report of Monitor** : Gives the summary of all the reports for that particular monitor.
- **Comparison Reports**: You can compare the attribute reports of various monitors within a particular monitor group. For eg., to compare the response time between monitors, click on *Response Time Reports* attribute link; from the list, select the monitors for which you need comparison. You can either select the time period for which the comparison is required or select the particular **Business Hours** for which the comparison is required. Currently, availability and health comparison reports are not supported.
- **At a Glance Reports**: The performance of top 10 monitors within the monitor group can be compared in a single view. For eg, in server monitor group, you can compare the performance of top 10 servers within the group. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute 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
- Custom Monitor Reports
- Trend Analysis Reports
- Server Reports
- Application Servers
- Database Servers
- Web Services Reports
- Web Servers Reports
- URLs/Web Apps Reports
- Middleware/Portal Reports
- Services Reports
- Mail Server Reports
- Java / Transactions Reports
- ERP Reports
- Custom Types

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.

Report Types	Details
Availability & Health	<p>Current Snapshot: The overall Availability and Health snapshot of Monitor Group and also the respective monitors in the Monitor Group.</p> <p>Critical Snapshot: The Availability and Health snapshot of monitors which are in Critical / Warning State in the Monitor Group.</p> <p>History: Availability and Health Outage reports for Monitor Group with details of Monitors that are in down state</p>

Report Types	Details
Availability Reports	<p>Percentage: The overall availability of the Monitor Group and the availability details for the respective monitors in the Monitor Group.</p> <p>Outage Comparison Report: With this report, you can compare the outages for current & past week / month. You would be able to find the details of how many times (count) outages have happened and also the duration of the outage. Also, you have the option to select the business hours for which you want the metrics to be calculated. You can define your custom business hours by using the Business Hours tool under Admin tab.</p> <p>Availability Trend Report: You have the history of 12 days, 12 weeks, 12 months availability report. Using this, you can follow the trend that is happening. Also, you have the option to select the business hours for which you want the metrics to be calculated. You can define your custom business hours by using the Business Hours tool under Admin tab.</p> <p>Availability and Downtime Trend Report: This section shows three reports - the availability of the monitor group in percentage, the downtime count, and the total downtime of the monitor group for the specified time period. The availability in percentage values are compared against the target availability to give you an idea of the availability trend of the specified monitor group. These information is also summarized in a table that shows the availability percentage, downtime count and the total downtime for the respective time periods.</p> <p>You can generate these reports for the last 12 days, last 12 weeks or the last 12 months. You can also generate these reports based on the business hour chosen. The business hours have to be defined using the 'Business Hours' tool under the 'Admin' tab. The reports thus generated can be exported as Microsoft Excel files (.xls).</p>
Health Reports	Percentage: The overall health of Monitor Group and the health details for the respective monitors in the Monitor Group.
At a Glance Report	The performance of top 10 monitors within this monitor group can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Alarm Summary	Alarm Occurrences for the application, attributes grouped in the application, and monitors, with graphical representation. Additionally, a graph representing the split up of total critical alarm occurrences in application by most critical monitors is also generated.
Monitor Group Attribute Report	The attribute report of the constituent monitors in the Monitor Group

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.

Parameters	Details
Attribute Details	<p>This contains the following details:</p> <p>Name of the attribute.</p> <p>The agent from which the attributes were added to the Custom Monitor.</p> <p>The port at which the agent is running.</p> <p>The type of the service or resource through which the JMX or SNMP agents are monitored.</p> <p>The minimum value obtained for every polling interval.</p> <p>The maximum value obtained for every polling interval.</p> <p>The average value of the attribute obtained for every polling interval.</p>
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.

Trend Analysis Reports

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

Report Types	Details
Downtime History	<p>Gives the downtime/uptime chart for "today"s period and also the downtime history for that particular monitor across all time periods.</p> <p>Also, you can view the summary details of Scheduled Downtimes and Unmanaged time. This will give you more clarity in knowing the monitor's exact downtime. You can also add notes on why the monitor was down for that particular time period.</p>

Report Types	Details
Summary Report	Gives the summary of all the reports for that particular monitor.
At a Glance Report	The performance of the selected monitors can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.

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.

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
At a Glance Report	The performance of top 10 Application servers can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Application server monitors, in milliseconds. (not for .NET)
Memory Usage	The minimum, maximum, and average JVM usage by all the Application server monitors, in bytes. (not for Oracle AS, .NET)
JDBC Connection Usage	The minimum, maximum, and average JDBC Connections of Application server monitors (not for Oracle AS, .NET, Tomcat)
Thread	The minimum, maximum, and average number of threads spawned by Application server monitors (not for Oracle AS, JBoss)
Session Details	The minimum, maximum, and average HTTP Sessions of Application server monitors (not for .NET, Tomcat, JBoss)

Report Types	Details
Request Throughput of Application Servers	Number of requests processed per unit of time in the server. (not for .NET, Tomcat, Websphere, JBoss, WLI, Weblogic)
Web Application Throughput of Application Servers	Number of requests processed per unit of time in the web application (not for .NET, Tomcat, Websphere, JBoss, WLI, Weblogic)

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.

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
At a Glance Report	The performance of top 10 database servers can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average time taken to connect to the database server by the Applications Manager server, in milliseconds.
Buffer Hit Ratio	The minimum, maximum, and average Buffer Hit Ratio of the database
Cache Hit Ratio	The minimum, maximum, and average Cache Hit Ratio of the database

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.

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
At a Glance Report	The performance of top 10 services can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Service monitors, in milliseconds.

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.

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager Mail Server Group.
At a Glance Report	The performance of top 10 mailservers can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Mail Server monitors, in milliseconds.

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.

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
At a Glance Report	The performance of top 10 servers can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Server Monitors, in milliseconds.
CPU Usage	The minimum, maximum, and average amount of CPU utilized by the Server Monitor.
Memory Usage	The minimum, maximum, and average amount of memory utilized by the Server Monitor.
Disk Usage	The minimum, maximum, and average amount of Disk space utilized by the Server Monitor.

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.

Health

The health of all the monitors in the Applications Manager server.

Report Types	Details
Availability	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.
At a Glance Report	The performance of top 10 web services can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Web Service monitors, in milliseconds.
Operation Execution Time	The time taken for getting response from the Service.

Web Server Reports

This generates reports for the Web 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 Web Server Monitor Type from the combo box). The following are the different Report types that are generated for the Web Server Monitor Type.

Health

The health of all the monitors in the Applications Manager server.

Report Types	Details
Availability	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 Server Monitors being monitored by the Applications Manager.
At a Glance Report	The performance of top 10 webserver can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.

Report Types	Details
Response Time	The minimum, maximum, and average response time of all the Web Server monitors, in milliseconds.

URLs/ Web Apps Reports

This generates reports for the URLs/ Web Apps 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 URLs/ Web Apps Monitor Type from the combo box). The following are the different Report types that are generated for the URLs/ Web Apps Monitor Type.

Health

The health of all the monitors in the Applications Manager server.

Report Types	Details
Availability	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.
At a Glance Report	The performance of top 10 webservices can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Web Service monitors, in milliseconds.

Middleware/Portal Reports

This generates reports for the Middleware/Portal 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 Middleware/Portal Monitor Type from the combo box). The following are the different Report types that are generated for the Middleware/Portal Monitor Type.

Health

The health of all the monitors in the Applications Manager server.

Report Types	Details
Availability	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.
At a Glance Report	The performance of top 10 webservices can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the Web Service monitors, in milliseconds.
JVM Usage	The minimum, maximum, and average JVM usage by the monitors
Connection Pool Usage	The minimum, maximum, and average JDBC Connections of the monitors
Thread Details	The minimum, maximum, and average number of threads spawned by the monitors
Session Details Time	The minimum, maximum, and average HTTP Sessions of the monitors

Java / Transactions Reports

This generates reports for the Java Runtime Monitor created using Applications Manager. The following are the different Report types that are generated:

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
At a Glance Report	The performance of top 10 java runtime monitors can be compared in

Report Types	Details
	a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average time taken to connect, in milliseconds.
Memory Usage	The minimum, maximum, and average amount of memory utilized
CPU Usage	The minimum, maximum, and average amount of CPU utilized

ERP Reports

This generates reports for the SAP Monitor created using Applications Manager. The following are the different Report types that are generated:

Report Types	Details
Availability	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.
Health	The health of all the monitors in the Applications Manager server.
CPU Utilization	The minimum, maximum, and average time taken to connect, in milliseconds.
Memory Utilization	The minimum, maximum, and average amount of memory utilized
Disk Utilization	The minimum, maximum, and average amount of disk utilized
PageIn Rate	The Average number of page-ins per second
PageOut Rate	The Average number of page-outs per second
Spool Utilization	Utilization of the spool work processes as a percentage
Background Utilization	Percentage of the background processing capacity currently utilized;
Front End Response Time	Average time that a user waits at the front end for the processing the request
Enqueue Requests	Number of lock requests

Report Types	Details
Connection Time	The minimum, maximum, and average time taken to connect, in milliseconds.

Custom Types

This generates reports for the Custom Monitors types created using Applications Manager. The following are the different Report types that are generated:

Report Types	Details
Availability	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 monitors in the custom monitor type being monitored by the Applications Manager.
Health	The health of all the monitors in the custom monitor type.
At a Glance Report	The performance of top 10 custom monitors can be compared in a single view. By clicking on the bars in the report, you can see all the attributes of the monitor in a single view. Further, you can drill down to see the individual attribute reports.
Response Time	The minimum, maximum, and average response time of all the custom monitors, in milliseconds.

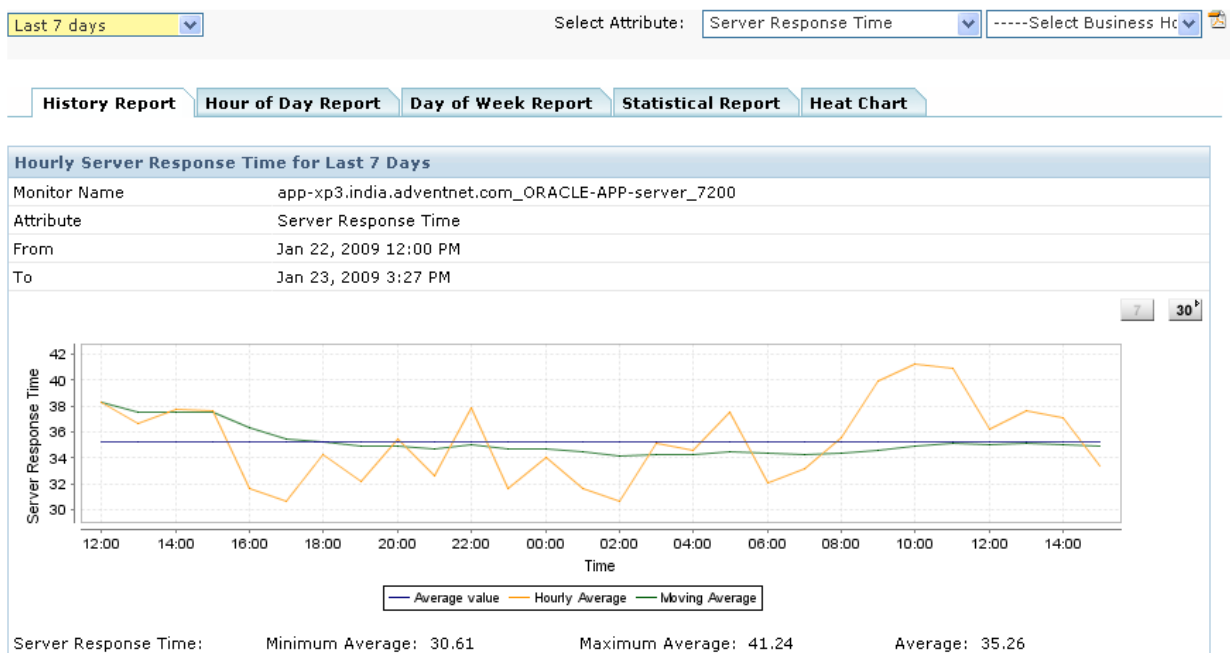
7 / 30 Reports

The **7/30 Reports** is available for various attributes/resource of a particular monitor. The 7/30 reports, apart from displaying availability for the past 7 days or 30 days, they also display the following reports for each attribute/resource. These reports can be exported into PDF formats.

- History Report
- Hour of Day Report
- Day of Week Report
- Statistical Report
- Heat Chart

History Report

History Report in Applications Manager provides detailed history of the particular attribute of a monitor. You can also generate history trend across business hours for a particular attribute. This provides you with an understanding to the amount of resources that has been utilized by the particular attribute over a period of time (week/month/year).



Archiving: All the data are archived and stored every one hour. Eg. Data from 10 AM to 11 AM are archived and marked as 11 AM when stored. If the monitor instance is completely down during the archiving interval of one hour, archiving will not take place for that hour.

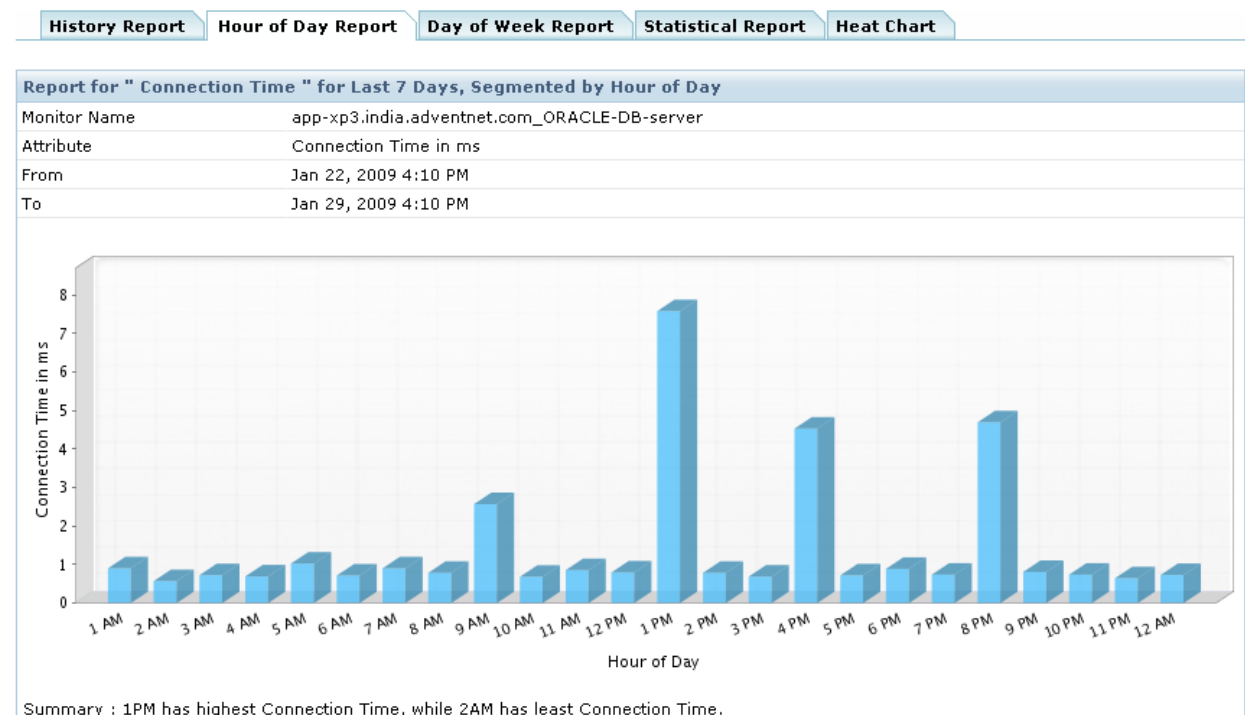
Minimum value: It represents the lowest value from the collected values in an hour. Eg. 6 on Sep 01, 2008 - 14:00 hours represents the lowest value '6' collected on Sep 01, 2008 between 13:00 and 14:00 hours.

Maximum value: It represents the highest value from the collected values in an hour. Eg. 12 on Sep 01, 2008 - 14:00 hours represents the highest value '12' collected on Sep 01, 2008 between 13:00 and 14:00 hours.

Hourly Average: It represents the average value from the collected values in an hour. Eg. 9 on Sep 01, 2008 - 14:00 hours represents the average value '9' collected on Sep 01, 2008 between 13:00 and 14:00 hours.

Hour of Day Report

A sample Hour of Day Report is shown below. This report generates hour's average for a particular time period (week/month/year) for the particular attribute. For example, if you have selected last 7 days data, the report generates hour's minimum, maximum and hourly average. This report helps you visualize the various bottlenecks that appear for this attribute / resource during a particular time period. This allows you to plan future impact of bottleneck on this attribute / resource.



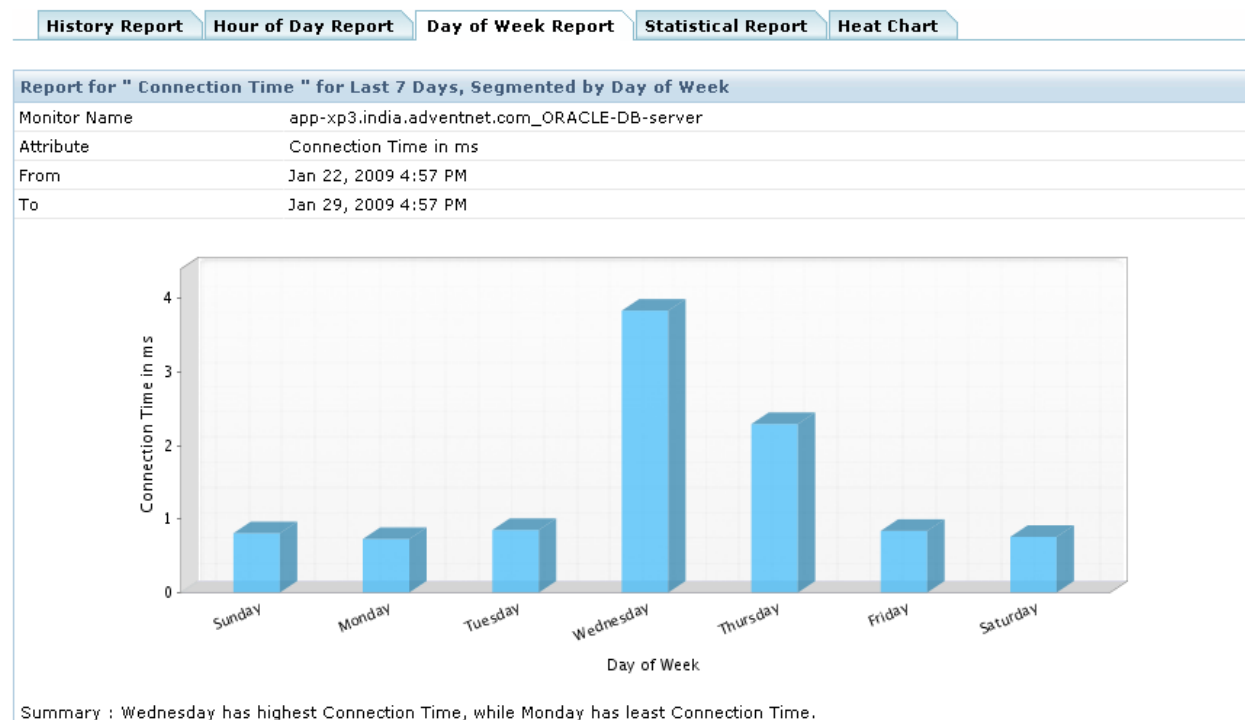
Minimum value: It represents the lowest value among the collected values in a particular hour of the day over a period of time. Eg. The lowest value '41' represents the data collected between 13:00 - 14:00 hours from Dec 4, 2008 3:55 PM to Dec 11, 2008 3:55 PM.

Maximum value: It represents the highest value among the collected values in a particular hour of the day over a period of time. Eg. The highest value '81' represents the data collected between 13:00 - 14:00 hours from *Dec 4, 2008 3:55 PM* to *Dec 11, 2008 3:55 PM*.

Hourly Average: It represents the average value of the collected values in a particular hour of the day over a period of time. Eg. The average value '62' represents the data collected between 13:00 - 14:00 hours from *Dec 4, 2008 3:55 PM* to *Dec 11, 2008 3:55 PM*.

Day of Week Report

A sample of Day of Week Report is shown below. This report generates average of a day for a particular time period (week/month/year) for the particular attribute. For example, if you have selected last 7 days data, the report generates everyday's minimum, maximum and hourly average and is shown below in this report. As shown in the graph below, the connection time for Oracle DB server has been highest for Wednesday and lowest for Monday. This implies that the traffic on Wednesday has been high when compared to rest of the days during the week. This would allow you to ensure that the connection time of Oracle DB server remains low for that particular day and help you troubleshoot performance issue quickly.



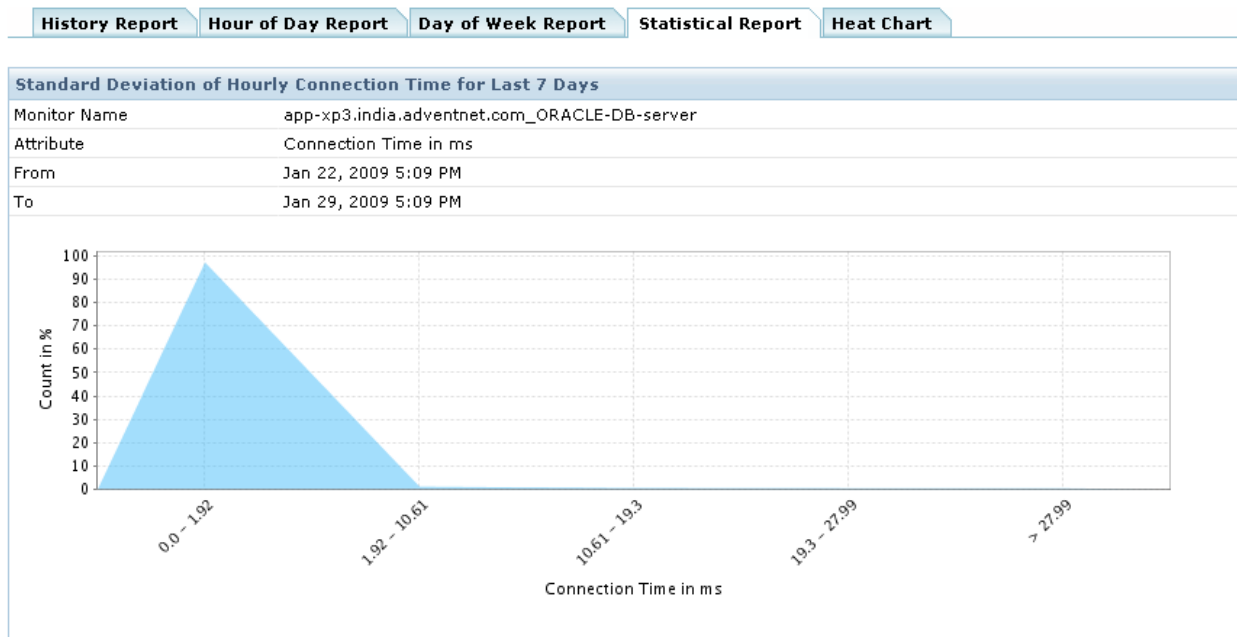
Minimum value: It represents the lowest value among the collected values in a particular day of the week over a period of time. Eg. The lowest value '41' represents the data collected on Wednesdays from *Nov 11, 2008 3:55 PM* to *Dec 11, 2008 3:55 PM*.

Maximum value: It represents the highest value among the collected values in a particular day of the week over a period of time. Eg. The highest value '81' represents the data collected on Wednesdays from Nov 11, 2008 3:55 PM to Dec 11, 2008 3:55 PM.

Hourly Average: It represents the average value of the collected values in a particular day of the week over a period of time. Eg. The average value '62' represents the data collected on Wednesdays from Nov 11, 2008 3:55 PM to Dec 11, 2008 3:55 PM.

Statistical Report

A sample Statistical Report is shown below. This report represents the standard deviation of this attribute over a period of time. For eg. lets consider CPU utilization attribute over a period of time. X-axis represents CPU Utilization range in percentage and Y-axis represents Count in percentage. Lets consider peak value of Count percentage to be 55% and is within the range of 70% - 80%. This means that for 55% of the polled value is within the range of 70% and 80%. This data can be used to re-allocate or organize resources for the server accordingly.



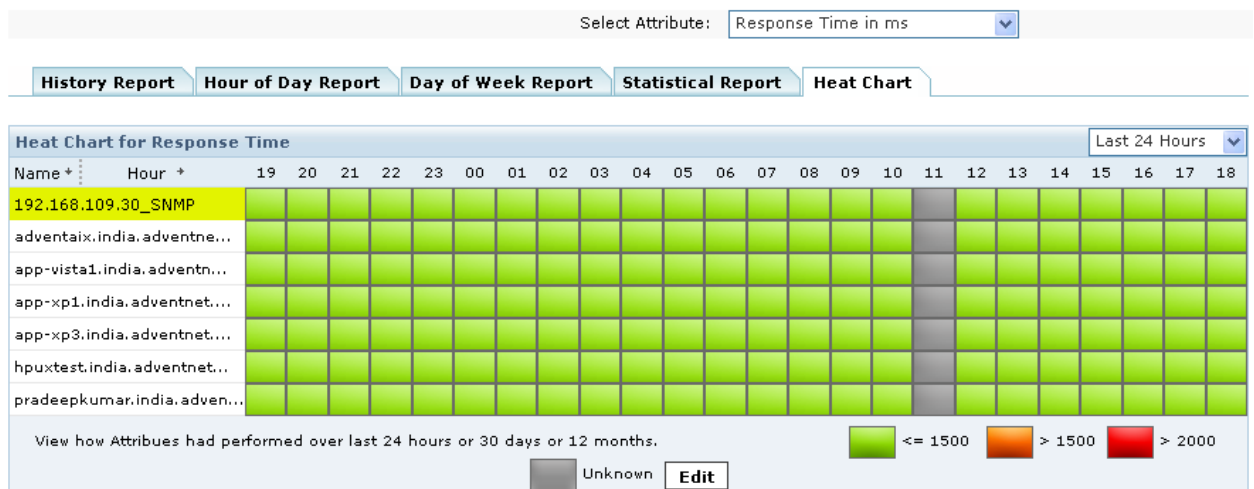
Heat Report

A sample Heat Report is shown below. This report is largely useful to compare the similar types of monitors and to check their performance of each monitor with other monitors. These heat charts are plotted based on how the attribute of the particular monitor type performs according to the threshold configured for that particular monitor. If a threshold is configured for the attribute of a particular monitor, then the threshold is taken and heat chart is plotted. There are three colors by which heat chart is plotted.

Red color indicates critical breach in threshold, Orange color indicates warning, and Green color is clear.

If the threshold is breached, then the color of the heat chart changes accordingly. This implies drop in performance, thus providing clear understanding of various monitors performance of the same type. If the threshold value for each attribute for that particular monitor is not set, then the common threshold value is automatically assumed and this heat chart is generated.

The **'Edit'** option provided in this chart will facilitate the user to view the heat chart in any other threshold definition on the fly. Please note that by editing threshold the view won't affect the original threshold configured for the attribute.



Top

Admin Activities

Performing Admin Activities

Applications Manager enhances effective business management allowing 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 the 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 Alarms
- Bulk Configuration of Monitors

Discovery and Data Collection:

- Bulk adding of Monitors
- Network Discovery
- Custom Monitor Types
- Performance Polling
- Downtime Scheduler
- Server Process Templates
- Windows Service Templates

Alarm/Action:

- Availability Settings
- Action / Alarm Settings
- Event Log Rules
- Alarm Escalation
- Global Trap Action
- SNMP Trap Listener

Applications Manager Server Settings:

- Global Settings
- Configure Mail Server
- Configure SMS Server
- Configure Proxy
- User Administration
- Add-On/Product Settings
- Product License
- Upload Files/Binaries
- Business Hours
- World Map
- Reports Settings
- Personalize Web Client
- Enable Reports
- REST API

Tools:

- Schedule Reports

Admin Activities:

- Data Backup
- Server Settings
- Production Environment

Discovery and Data Collection

The discovery and data collection module contains settings related to application and server discovery as well as data collection from monitors.

The topics covered in this section are:

- Bulk Import of Monitors
- Network Discovery
- Custom Monitor Types
- Performance Polling
- Downtime Scheduler
- Server Process Templates
- Windows Service Templates

Bulk Import of Monitors

Selecting this option, you would be able to add monitors of the same type in bulk. By giving all the configuration details in a **.csv file**, bulk import of monitors is made possible.

Bulk Import of Monitors:

Click on **New Monitor link**, select the monitor type you want to add. In the New Monitor screen, you will find the link to **Bulk Import Monitor**. Clicking on that link will take you to Bulk Import Monitor screen. Here, you can **upload the .csv file** that has all the configuration details. The file would be uploaded to the Applications Manager Machine in the location *<Product-Home>\working\bulkadd\<particular.csv>*. This file will be deleted once the discovery for monitors is scheduled, for security reasons. The list of all monitors to be added is listed down. On clicking '**Start Discovery**', all the monitors would be added to Applications Manager.

Format for Bulk Import .csv file

Monitor Type	Details
Servers	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,OperatingSystem,SubNetMask,ModeOfMonitoring,UserName,Password,SNMPCommunityString,TelnetSSHCommandPrompt,MonitorGroup,PolllInterval</p> <p>**MonitorGroup,PolllInterval entries are optional</p> <p>* OperatingSystem can have the following values : Windows 2003 or Windows 2000 or windows XP or WindowsNT or AIX or FreeBSD or HP-UX or Linux or Mac OS or Solaris or HP-TRU64.</p> <p>* ModeOfMonitoring can have the following values : WMI or SNMP or SSH or TELNET .</p> <p>* Download an Example csv File for Servers.</p>
JBoss	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,JBOSSTVersion,Username,Password,isSSEnabled,MonitorGroup,PolllInterval</p> <p>**MonitorGroup,PolllInterval entries are optional</p> <p>* JBOSSVersion can have the following values : 3.2.x or 4.x or 4.0.1 or 4.0.2.</p> <p>* Download an Example csv File for JBoss.</p>
Microsoft .Net	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,UserName,Password,MonitorGroup,PolllInterval</p> <p>**MonitorGroup,PolllInterval entries are optional</p> <p>* UserName and Password should be the credentials of user with Administrator privileges.</p> <p>* Download an Example csv File for Microsoft .NET.</p>

Monitor Type	Details
Oracle AS Server	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask, Port,MonitorGroup,PollInterval</p> <p>**MonitorGroup,PollInterval entries are optional</p> <p>* Download an Example csv File for Oracle AS.</p>
Tomcat	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,TomcatVersion, isSSLEnabled,UserName,Password,MonitorGroup,PollInterval</p> <p>**MonitorGroup,PollInterval entries are optional</p> <p>* TomcatVersion can have the following values : 3.x or 4.x or 5.x or 6.x.</p> <p>* Download an Example csv File for Tomcat.</p>
WebLogic Integration	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,WeblogicIntegrationVersion, Username,Password,MonitorGroup,PollInterval</p> <p>**MonitorGroup,PollInterval entries are optional</p> <p>* WeblogicIntegrationVersion can have the following values : 8.x .</p> <p>* Download an Example csv File for Weblogic Integration.</p>
WebLogic Server	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,WeblogicVersion, Username,Password,MonitorGroup,PollInterval</p> <p>**MonitorGroup,PollInterval entries are optional</p> <p>* Weblogic_Version can have the following values : 7.0 or 8.1 or 9.x .</p> <p>* Download an Example csv File for Weblogic Server.</p>
WebSphere Server	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,port,WebsphereVersion,SOAPPort, UserName,Password,DeploymentMode,NetworkDeployerHost,NetworkDeployerSOAPPort, MonitorGroup,PollInterval</p> <p>**MonitorGroup,PollInterval entries are optional</p> <p>* Each monitor information should be given in the order of the fields specified in the Header.</p> <p>* WebsphereVersion can have the following values : 5.x or 6.x</p> <p>* DeploymentMode can have the following values BASE or ND.</p> <p>* Download an Example csv File for Websphere Server.</p>
IBM DB2	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,Username,Password, DatabaseName,MonitorGroup,PollInterval</p> <p>* Download an Example csv File for DB2.</p>

Monitor Type	Details
MS SQL	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,UserName>Password, InstanceName,MonitorGroup,PolIInterval</p> <p>**MonitorGroup,PolIInterval entries are optional</p> <p>* If you want to connect using Named Instance specify the field InstanceName .If not please leave this field empty.</p> <p>* Download an Example csv File for MS SQL.</p>
MySQL	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,UserName>Password, DatabaseName,MonitorGroup,PolIInterval</p> <p>**MonitorGroup,PolIInterval entries are optional</p> <p>* Each monitor information should be given in the order of the fields specified in the Header.</p> <p>* Download an Example csv File for MY SQL.</p>
Oracle	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,UserName>Password, InstanceName,MonitorGroup,PolIInterval</p> <p>**MonitorGroup,PolIInterval entries are optional</p> <p>* Download an Example csv File for Oracle.</p>
Sybase	<p>Format for the Bulk Import csv file :</p> <p>#Header: DisplayName,HostName,SubNetMask,Port,UserName>Password, DatabaseName,MonitorGroup,PolIInterval</p> <p>**MonitorGroup,PolIInterval entries are optional</p> <p>* Download an Example csv File for Sybase.</p>
URL Monitor	<p>Format for the Bulk Import csv file :</p> <p>#Header:</p> <p>DisplayName,URLAddress,CheckForContent,ErrorIfMatch,UserName>Password, TimeoutInSeconds,FormSubmissionMethod,MonitorGroup,PolIInterval</p> <p>**MonitorGroup,PolIInterval entries are optional</p> <p>* Each monitor information should be given in the order of the fields specified in the Header.</p> <p>* FormSubmissionMethod can have the following values : post or get</p> <p>* The attributes</p> <p>CheckForContent,ErrorIfMatch,UserName>Password,TimeoutInSeconds,FormSubmissionMethod are all optional.</p> <p>* For Example a simple form of monitor can just have</p> <p>#DisplayName,URLAddress,CheckForContent.</p> <p>* Download an Example csv File for URL Monitor.</p>

Discovery

Network Discovery

Services

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

To discover all the Monitors in a network:

1. Click the **Admin** module tab.
2. Click **Discover a Network** under **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 Monitors 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**.

Some **FAQs** regarding Network Discovery

1.How does "Network Discovery" function work? How to discover the network? Eg.Through what mode?

Initially Applications Manager get all the Ip addresses in the given domain and then Applications Manager discovers them by using ping test. If the ping test succeeds and if SNMP agent is running on that machine, Applications Manager will try to add it to the appropriate category (i.e., windows / linux / solaris) and collect data, otherwise Applications Manager will add that server to unknown category.

2. If I add a new "Network Discovery", does it only discover once or discover at regular intervals? Because there are only "Add New" and "Disable Network Discovery" buttons, I don't know when it will start to discover and when it will finish discovery.

When you add Network Discovery, it will rediscover the network every time you restart Applications Manager and also it will do rediscovery once in every 24 hours. Once you start network discovery, it will start discovering the servers in the network. It will wait for 20 seconds interval between discovering servers.

3. I find "Network Discovery" can find a small part of the monitors in the network only, there are lots of monitors that can't be found.

In the professional trial version of Applications Manager, only 50 servers are discovered using Network Discovery.

4. I don't want to monitor a certain monitor, I delete it manually; but I don't disable network discovery, will it be discovered and monitored again?

Yes, it will discover that monitor again in the next rediscovery which takes place after 24 hours.

 [View Related Blog](#)

Services

Using this option, you can choose which of the services needs to be monitored by default. The services are listed down along with their default ports. For eg., if you had already added a Windows Server monitor, by using this option, you can choose the services (that are running in that windows server) to be monitored. You choose to monitor all the tomcats & IIS servers that are running in the windows server. Data Collection does not happen for services that are not enabled, thereby increasing the efficiency of monitoring in general.

By using the edit option, you can edit the port number. If there are multiple ports, enter the ports as comma separated.

See Also

- [New Monitor](#)

Custom Monitor Type

By using this option, you can define your **own monitor types** apart from the monitor types that are available by default.

This feature allows to associate a monitor type to the inhouse scripts that might be used for monitoring your own applications. For eg., if you are using various scripts to monitor Siebel CRM, you can now associate these scripts and model Siebel as one of the monitor types. Thereby having robust out of the box support for monitoring Forum Software, build Business Intelligence Dashboards, monitor Custom Application Log Files on multiple servers etc.

Custom Monitor Demo: Have a look at the demo that helps you to add a new Custom Monitor Type

WorkFlow

Step1) The custom monitor type helps you create and define *metrics / attributes* that will be tracked.

Step 2) Then specify a script (Linux Shell Script / Windows Batch File) that needs to be executed to get the data and provide it to Applications Manager in the appropriate format.

In these scripts users can use any mechanism to get the data. For example users can :

- Invoke a Java Program, PHP, Python Scripts etc and make database calls to pull data and feed it to Applications Manager
- Can make native calls to other programs and pipe the data to the output file
- Parse Log Files and give a summary of metrics as the input to Applications Manager

Creating New Monitor Types:

You can create new monitor type by clicking on the 'New Monitor Type' link inside the *New Monitor* link or by clicking on the *Custom Monitor Types icon* under *Admin* tab.

- Enter the *Monitor Type* name
- Select Base type - Currently, scripts are the base to build new monitor type.
- Select the Monitor Type *Category* - For eg., If you are monitoring postgresql using in-house scripts, you can add postgresql monitor type and you can place it under Database category

Define the **attributes** you want to monitor

- Enter the String Attributes that you want to monitor - Enter the attributes line by line.
- Enter the Numeric Attributes that you want to monitor - Enter the attributes line by line.
- You can monitor the output in a *table format*, enter the Table Name, Numeric attributes, Sting attributes, Unique column and Column delimiter. More help
- Click on *Create Monitor Type* to finish the configuration of new monitor type.

Now, you have defined a custom Monitor type. The next step would be to create instances & associate them to the new monitor type defined.

[Script Monitor Overview: Based on the polling interval, Applications Manager executes the script to be monitored. The script will transfer its output to another specific *Output File* configured. The output of the script should be in a Key=Value format where '=' can be any delimiter. Applications Manager parses the Output File and executes the actions configured]

Adding Custom Monitors:

- In the *User Created Monitor Type* screen, the newly created monitor types are listed down. Click on the *Add New* icon to add the monitors
- Add New monitor screen opens up, Select the custom monitor type from Monitor Types drop down box. [For eg., Siebel]
 - Enter the Display Name.
 - Choose the location of script that you want to monitor - Local or Remote.
 - Specify the absolute path of the script.
 - Specify the absolute path of the execution directory.
 - Specify the absolute path of the Output File
 - Enter the arguments that needs to be passed.
 - Enter the polling interval and timeout.
 - Click Add Monitor(s)

You have already given the attributes to be monitored as common to all monitors under custom Monitor Type. So there is no need to give input attributes to be monitored again

- Upon adding the custom monitors, you can see the performance attributes in the monitor details page.

Usage Scenario 1: Creating New Siebel Monitor Type

One customer had 6 Siebel applications running in 6 different machines. As, out of the box support for Siebel Application is not available, he uses the Script Monitoring feature of ManageEngine Applications Manager to monitor his applications. He has identical scripts running in the 6 machines and they produce the same output in the output file in the respective machines. Now he configures them as six Script Monitors. This gives him an opportunity to monitor his Siebel applications. Using Script Monitor facility, he monitors the following attributes

- transaction Router
- server request processor
- transaction processor

There are few disadvantages in his usage.

1. He has to give the same Output details while specifying the same six applications.
2. If he has to edit / add / delete the attributes , then he has to do so in all the 6 Script Monitors.
3. Further he would like to see them as 6 Siebel Monitors rather than 6 Script Monitors.

Here comes the usage of New Monitor Type, that would avoid all the above inconveniences.

1. Output Settings can be specified only once. You could specify the Scalar String / Numeric attributes and tabular settings only once while defining the type, say Siebel.
2. You could create any number of monitor instances for that particular type , just like any other in-built type say SAP / Weblogic / Oracle monitors in Applications Manager. While doing so, you just need to specify the Hostname and the corresponding Scripts
3. Adding / Deleting / Modifying attributes of some particular monitor type commonly will affect all the monitors of that monitor type.
4. Now you will be seeing 6 Siebel monitors rather than 6 Script Monitors.
5. Reports can be enabled for this type like any other type.

The same concept can be applied to any other application say for monitoring People Soft applications.

Usage Scenario 2: Business Intelligence Dashboard

Users can build custom **Business Intelligence dashboards** and have it reported and alerted on.

Some possible metrics could be

- Call Volume in the last one Month
- Time taken to finish a call
- Number of simultaneous Calls

Usage Scenario 3: Custom Application Log Files

Some metrics that you can add with a little bit of coding are :

- Number of security breaches
- Number of Errors During Login etc.

Managing Custom Monitor Types:

You can edit the configuration of the Monitor types by clicking on the **Custom Monitor Type** link under **Admin Tab**. It opens up to list all the User created Monitor Types. From here you add new monitors to the custom monitor types, edit the configuration and more importantly **enable or disable reports** of these custom monitor types.

Performance Polling

Data Collection

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.

Servers

Using this option, Disk IO Stats can be Enabled or Disabled for the servers. On enabling the option, Data Collection will happen for Disk IO stats and you can see the details of Disk IO Stats in the Server details page. If it is not enabled, Data Collection will be stopped for Disk IO Stats.

This option is available for IBM AIX, Linux and Solaris servers.

Oracle

Using this option, You can Enable or Disable Data Collection for Disk Reads, Buffer Gets and Lock and Wait Statistics for Oracle servers.

On enabling the option, Data Collection will happen for Disk Reads, Buffer Gets and Lock and Wait Statistics and you can see the details of Disk IO Stats in the Oracle details page. If it is not enabled, Data Collection will be stopped for Disk Reads, Buffer Gets and Lock and Wait Statistics.

WebLogic

Using this option, You can Enable or Disable Data Collection for Wep Applications, EJBs and Servlet Statistics for Weblogic servers. The list of Weblogic servers are displayed by selecting the checkbox. Data Collection will happen for the Weblogic components that are displayed under the corresponding Enable listbox.

By default, EJB and Servlet Data Collection are disabled. You can enable Data Collection for EJB and Servlet by selecting the Weblogic server from Disable list box and move it to the Enable listbox and save the configuration.

MS SQL

Using this option, You can Enable or Disable data collection for Scheduled jobs and Database backup.

By default, they are disabled.

My SQL :

Using this option, You can Enable or Disable Data Collection for Database Tables, to takes place Once in a Day.

By default, The Datacollection takes place for every polling.

You can Enable/Disable datacollection for Database Tables by selecting the *"Collect Database tables information once in Day"* checkbox and save the configuration.

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
- Once

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 **Once**.
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.

Server Process Templates

A server process template is a pre-defined reusable collection of processes. It provides an easy way to add multiple processes for monitoring across a group of servers. For example, if you want to monitor the 'init' process in all your Linux servers, you can configure a server process template for this process and apply the template across all your Linux servers. This is better than manually adding the 'init' process in your Linux servers one by one.

Steps to Add a New Server Process Template:

1. Click **Server Process Templates** link under Admin tab.
2. Specify **Template Name** and **Description**.
3. Click **Add Process** link to add processes for monitoring. You can either *Manually Enter the Process Details* or *Choose Process Details from Available Servers*.
 1. If you opt for the first option, specify the Process Name and Arguments.
 2. If you opt for the second option, select the appropriate monitor type and the monitor(s), and click the *Show Process* link. All the processes running in the servers will be listed. Select the necessary process from the list and click OK
4. If you want to receive notifications when the threshold values of the process attributes are violated, you have to **Configure Alarms for Attributes**. The attributes of the process will be listed on the left-hand side. Click the *Associate* link corresponding to the attribute to open the *Configure Alarms* screen.
 1. Select the necessary threshold from the *Associate Threshold* list box.
 2. You can also *Associate Actions* for the thresholds if necessary. Choose the necessary action from the Available Actions list and add them to the Associated Actions list. By default, you can associate action for critical severity. If you want to associate actions for warning and clear severities, click the *Show Advanced Options* checkbox, and select the appropriate actions from the list.
 3. Click Add to Template button once you have configured the thresholds and actions.
5. You can apply your process and threshold configuration under the **Associate Configuration to Monitors** section. You can either apply the configuration to monitor types or choose from a list of monitors or apply to specific monitor groups.
 1. To apply the configuration to specific monitor types, choose the *Apply to Monitor Types* option. The server types available in your Applications Manager installation will be listed below. Choose the required server type to apply the template to all servers of that type.
 2. To apply the template to individual monitors, choose the *Apply to Monitors* option and choose the necessary monitor(s) from the list.
 3. To apply the template to monitor groups, choose the *Apply to Monitor Groups* option and select from the monitor groups listed.
6. Click **Save Template** to complete your server process template configuration.

Windows Service Templates

A Windows service template is a pre-defined reusable collection of Windows services. It provides an easy way to add multiple services for monitoring across a group of Windows servers. For example, if you want to monitor the 'EventLog' service in all your Windows XP servers, you can configure a Windows service template for this service and apply the template across all your XP servers at once. This is better than manually adding the 'EventLog' service in your Windows XP servers one by one.

Steps to Add a New Windows Service Template:

1. Click **Windows Services Templates** link under Admin tab.
2. Specify **Template Name** and **Description**.
3. Click **Add Service** link to add services for monitoring. You can either *Manually Enter the Service Details* or *Choose Service Details from Available Servers*.
 1. If you opt for the first option, specify the Service Display Name and Service Name.
 2. If you opt for the second option, select the appropriate monitor type and the monitor(s), and click the *Show Service* link. All the services running in the servers will be listed. Select the necessary service from the list and click OK.
4. If you want to receive notifications when the threshold values of the service attributes are violated, you have to **Configure Alarms for Attributes**. The attributes of the service will be listed on the left-hand side. Click the *Associate* link corresponding to the attribute to open the *Configure Alarms* screen.
 1. Select the necessary threshold from the *Associate Threshold* list box.
 2. You can also *Associate Actions* for the thresholds if necessary. Choose the necessary action from the Available Actions list and add them to the Associated Actions list. By default, you can associate action for critical severity. If you want to associate actions for warning and clear severities, click the *Show Advanced Options* checkbox, and select the appropriate actions from the list.
 3. Click Add to Template button once you have configured the thresholds and actions.
5. You can apply your service and threshold configuration under the **Associate Configuration to Monitors** section. You can either apply the configuration to monitor types or choose from a list of monitors or apply to specific monitor groups.
 1. To apply the configuration to specific monitor types, choose the *Apply to Monitor Types* option. The server types available in your Applications Manager installation will be listed below. Choose the required server type to apply the template to all servers of that type.
 2. To apply the template to individual monitors, choose the *Apply to Monitors* option and choose the necessary monitor(s) from the list.
 3. To apply the template to monitor groups, choose the *Apply to Monitor Groups* option and select from the monitor groups listed.
6. Click **Save Template** to complete your Windows service template configuration.

Alarm/Action

This module contains settings related to availability of monitors as well as settings related to fault management options.

The topics covered in this section are:

- Availability Settings
- Action/Alarm Settings
- Event Log Rules
- Alarm Escalation
- Global Trap Action
- SNMP Trap Listener

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.

Clear Health Alert during Maintenance Period

When you schedule a downtime or unmanage a monitor, it will show the last health status. If the monitor is down before a downtime or maintenance, it will be displayed as 'Down'.

If you choose this option, then Applications Manager will clear the last health status of the monitor.

Check for Network Availability

When 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 alarms 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, alarms 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 (and false alarms) by enabling the '**Check URL Availability**' option.

When this option is enabled, Applications Manager will generate alarms for the unavailability of URL only if the other specified URL - reference URL is not down. For eg, 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 say for eg., google.com which is expected to be up always. Now,

Applications Manager tries to monitor URL for its availability. If not available, it checks reference URL, if the reference URL is available the alarms are generated. If the reference URL itself is not available (meaning the machine is out of network or any such case) false alarms are not generated and URL is not shown as down. Further a mail is sent to the configured mail address intimating the same.

 [View Related Blog](#)

Availability Timeout Check

Using this option, you can set timeout for checking availability globally.

Action / Alarm Settings

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

General:

Enable Actions

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

Execute Actions Repeatedly

If you want the actions to be triggered continuously during every poll, till alarms 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.

Email

By selecting this option, you can add the server snapshot - Dial view as an inline attachment in the alarm Email. This option is available only if the Health becomes critical.

Monitor Error Mail

By selecting this option, you can send emails in case of any fatal monitor error like data collection not happening, etc. This mail will be sent to the email address specified in the 'admin' user account. If no email address is specified, the mail will be sent to the email address specified in the 'Mail Server' settings, hence ensure that you specify a valid email address.

Furthermore, you can specify the number of times the error has to occur before email is triggered in the *Check for consecutive polls before sending error* box.

Date Format

Using this option, you can set the required date format in the Email alarms. It can either be

Day Mon dd HH:mm:ss IST yyyy (Default) - Thu Feb 22 12:02:40 IST 2007

or

MM/dd//yyyy HH:mm:ss - 02/22//2007 12:02:40. See Replaceable tags for usage of **\$Date**.

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.

Dependency:

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.

Consecutive Polls before Reporting an Error:

The Critical, Warning, and Clear alarms are generated based on attributes that you have configured. You have control over the alarms that are being generated. Simply specify the number times after which the alarm 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 Action / Alarm settings, Polls before reporting an error, can be configured for threshold and availability of individual monitors. Refer Configuring Consecutive Polls.

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 alarms 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 alarm 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

To add new event log other than what are available by default, click the option "*Add New Event Log*" in the right hand bottom corner of the web client.

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 alarm severity.

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

Alarm Escalation

Applications Manager provides an option to configure rules which ensure that any alarm that lies unattended for a while is brought to the notice of the IT administrator. This ensures that all critical alarms are taken care of before it gets late.

For more information on alarm escalation, refer this section.

Configure Global SNMP Trap

You can configure Global SNMP Trap action in Applications Manager to send alerts to SNMP trap listeners. The alerts generated can be viewed from SNMP trap listeners at the corresponding destination address and port.

Follow the steps given below to create a global SNMP Trap action:

1. Click '**Global Trap Action**' under Admin tab. It takes you to '**Create Global Trap Action**' page.
2. Select the **SNMP Trap Version** from the drop-down box. You can select either v1 or v2c.
3. Enable or disable the action by choosing the appropriate radio button under **Status**. By default, the 'disable' button is selected.
4. Specify the hostname where the SNMP Trap listener is running under **Destination Address**
5. Specify the port at which traps are received in the **Destination Port** field.
6. Enter the **Community String** of the trap. The default value is 'public'.
7. Click **Create Action** button to complete the configuration.

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 alarms 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 alarm 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 AppManager Home/Conf directory. Restart the server for the changes to take effect.

Follow the steps given below to add a SNMP Trap Listener.

1. Click the **Add New** option in SNMP Trap Listener under the Admin Tab. This will take you to the **Add SNMP Trap Listeners** page.
2. Enter the **Trap Listener Name**.
3. Choose the **Status** of the trap. The Status is 'enable' by default.
4. Select the **SNMP Trap version**, either v1 or v2c.
 1. If you select **v1**, select the **Generic Type**. The various generic types are coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss, and enterpriseSpecific. If you select enterpriseSpecific type, you can also provide wildcard symbol ' * ' or numeric value for **Specific Type** field.
 2. Enter the **Enterprise OID**. You can use the MibBrowser to get the Object ID. If you select a Parent OID from the MibBrowser, all child OIDs will also be automatically listened.
 3. If the version is **v2c**, then enter the **Trap OID**. You can use the MibBrowser to get the Object ID.
5. Select the **Severity**. It can be Clear, Warning, Critical or New Threshold Profile. If you select the 'New Threshold Profile' option, you have to specify the threshold name and the conditions for the different severities of alarms. By default, you can configure the condition for *Critical* severity. Select the 'Show Advanced Options' checkbox to configure *Warning* and *Clear* alarm severities.
6. Trap can be received from any Host or you can specify the Host from which the trap can be received.
7. **Associate Actions** that need to be executed when the trap is received. The actions can be chosen from the list of actions configured. If you have selected the 'New Threshold Profile' option under Severity, you have to associate the actions for the severities defined in the threshold profile.
8. **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 alarms configured for the traps received can be viewed from the Alarms Tab.

Note: Dell OpenManage can be integrated with ManageEngine Applications Manager via the SNMP Trap Listener. More in Application Manager's blog.

Applications Manager Server Settings

The topics covered in this section are:

- Global Settings
- Configure Mail Server
- Configure SMS Server
- Configure Proxy
- User Administration
- Add-On/Product Settings
- Logging
- Personalize Web Client

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 Intro Tab

When you login into the Web Client, an Introduction page is displayed to help novice users to get started and to understand the terms used in the product. If you want the Introduction page to be displayed every time you login, select this option.

Do not hide Advanced configuration in Alarm Configuration

By selecting this option, you can always have all the advanced options expanded by default in the "Configure Alarms" 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 & alarms.

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.

Add Host also when you add a new service

While adding a service as Monitor, by selecting this option, the host on which the service runs will also be added.

Restart the product in case of serious server error

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

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

Show inline feedback form

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

Enterprise Edition Settings

You can convert the standalone professional server to Managed Server by giving the Admin Server Host name and SSL port. Note: This option is available only if you have installed the full build and does not work for upgrades through PPM.

Collect Usage Statistics

Applications Manager collects statistical data associated with quality, stability, and usability of the product.

By checking the **Enabled** option you grant permission to collect this data. The data collected will remain confidential and be used during analysis.

Configure Mail Server

Mail servers are configured to send EMail to desired destinations. For instance, when you perform an action to send EMail for some alarms, 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. For TLS Support in the mail server configuration, select **TLS Authentication Enabled** option.
5. Click **Save** to save the configurations.

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

Note: To verify, SMTP access for Gmail from your Applications Manager installed system, you will need to run a telnet test, which will check that your computer can contact gmail SMTP servers. Enter *telnet smtp.gmail.com 465* (or 587) and check for any response. In case you fail to receive a response, we recommend contacting your system administrator to get the access.

If the chosen mail server is down for some reasons, you have an option to configure a **Secondary Mail Server** that functions as a back up mail server. Provide the SMTP server name & the Port number. Provide the user name and password, if the SMTP server requires authentication.

Configure SMS Server

SMS Server should be configured for sending SMS alarms via Modem. Available in Windows only.

SMS Servers Settings:

Prerequisites:

- Connect your GSM Modem to the **Serial Communication Port**.
- Know the Modems that are supported - [Link](#)
- Only a **serial cable** must be used for connectivity

Enter the **Port Number** to which Modem is connected: For eg. COM3 . To find the Port Number - Click on *My Computer*->right click *Properties*->*Hardware*->*Device Manager*->*Ports (COM & LPT)* under ->*Prolific USB-to-Serial Comm Port (COM3)*.

The Modem Status details that would be displayed are

Details:

- Modem Manufacturer
- Modem Model
- Battery Status
- Signal Status
- Status

Configure Proxy

In situations where any URL to be monitored is available in the Internet, then the requests have to be routed through a HTTP proxy server. Such URL monitoring can be performed by setting the proxy configuration. For eg., to access websites from your browser, you should configure an HTTP Proxy (In Internet Explorer, Click on Tools >Internet Options > Connections > LAN Settings). Follow the steps given below to configure a proxy server:

1. Open Web Client, click on Admin tab, then 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.

The entries may be any of the following:

a complete host name (e.g. "www.zohocorp.com")

a domain name; domain names must begin with a dot (e.g. ".zohocorp.com")

an IP-address (e.g. "12.34.56.78")

an IP-subnet, specified as an IP-address and a netmask separated by a "/" (e.g. "34.56.78/255.255.255.192"); a 0 bit in the netmask means that that bit won't be used in the comparison (i.e. the addresses are AND'ed with the netmask before comparison).

4. Click **Save**.

All request to the Internet will then be routed through the proxy server.

User Administration

Applications Manager permits four 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. To delete a user, you should have logged in as default Administrator.

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.

Note:**Permissions:**

Using the Permissions options, you can allow Operators to manage / unmanage monitors, reset the status of monitors, edit display names and also to execute actions. Otherwise, the admin user has permission to perform these activities. Also, permission can be given to Admin or operator to use the Telnet client of the server monitor, if the server was added in Telnet & SSH mode. AS400 Permissions allow you to permit Operators to execute AS400 Admin activities.

View:

This is for Operator only. Using View option, you can define how to represent your subgroup in the webclient. You can either show the associated subgroups directly in the home tab itself or from the corresponding top level Monitor Group.

Account Policy:

To enhance Web Client security, Account Policies can be configured. You can define the number of continuous failed login attempts to lock user account and Idle session timeout. You can enforce single user session and strong password rules.

Strong password rules

Note :

- Password cannot be same/part of your Login name
- Password length should not be less than 8 character
- Password length should not be greater than 255 character
- Password should contain atleast 1 numeric character
- Password should contain atleast 1 special character
- Password should contain both uppercase and lowercase character
- Password should not be same as your last 4 password(s)

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**.

AD Authentication and Capability to import users from Active Directory

Setting up of user accounts, passwords, and assigning privileges to different roles manually, while assuring security is a time-consuming task. We require a more convenient method to add a large number of users to Applications Manager.

Active Directory Authentication Module is implemented in order to ease the user administration in Applications Manager. Using Active Directory(AD) authentication module you can import users from Active Directory to Applications Manager. Active Directory authentication enables users to log in to Applications Manager if they have an account in an Active Directory domain.

Users imported from the Active Directory can login into Applications Manager using their Active Directory credentials. This removes the users' burden of remembering yet another username & password for Applications Manager alone.

Since Active Directory authentication is done in the Domain Controller all the account policy regulations of the company/domain is automatically inherited to Applications Manager credentials also.

How to Import Users from Active Directory

To import users from Active Directory, use the following steps:

1. Click on the **Admin** tab.
2. Under the **Applications Manager Server Settings** click **User Administration** to see a list of User Profiles.
3. Click the **Add New** link under the list of user profiles to come to the **New User** page.
4. Click on the new tab called **Import Users from Active Directory**.
5. Select a domain name from the drop-down list.

You can select an already added domain from the drop-down list or add a new domain. You can also edit the existing Domain controller settings in the same manner.

Adding a New Domain

1. Select the **Add New Domain** option from the **Domain Name** drop-down list.
2. Enter the following details:

Domain Name: Name of the domain from where the users need to be imported.

Domain Controller: The hostname or the IP address of the DNS server for the domain.

Username: Active directory username of the domain user in DOMAIN\username format

Password: Active directory password of the domain user.

Search Filter: To filter out search result you can use characters followed by * as well as the role criterion in LDAP search filter format. These search filters use one of the following formats <filter>=(<attribute><operator><value>) or (<operator><filter1><filter2>).

For example: "(&(objectCategory=person)(objectClass=user)(!cn=andy))"- All user objects but "andy".

3. Click on **the Fetch Users from AD** button to import users from the active directory.
4. When the list of existing users is displayed select the user(s) to be added, assign roles and click on **Add Users** to add the users.
5. In the new **Import Users** tab from Active Directory pop-up window select the users that you wish to add from the drop-down list.
6. Assign a role - Operator, User, Administrator or Manager to each of the users.
7. Click on the **Add User** button to import the user to Applications Manager or click on **Add Users And Configure Another** to add more users.

You can edit User Profiles from the list of users.

Add-On/Product Settings

- **ManageEngine ServiceDesk Plus**
- **ManageEngine OpManager**
- **ManageEngine OpStor**

ManageEngine ServiceDesk Plus

ManageEngine 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 alarms, from Applications Manager . So, besides the provision to email, sms, and notification of alarms in other forms, the alarms can also be tracked by logging trouble tickets to ServiceDesk Plus. This helps in issue tracking.

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.

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 alarm should be associated to the Ticket Action, to log a trouble ticket to ServiceDesk Plus

ManageEngine OpManager Network Monitoring Connector **Add On!**

ManageEngine Applications Manager integrates with a comprehensive Network Monitoring Tool, ManageEngine OpManager. To know more about how to configure ManageEngine OpManager Network Monitoring Connector Click [here](#).

ManageEngine OpStor SAN Monitoring Connector [Add On!](#)

ManageEngine Applications Manager integrates with Storage Device Monitoring Tool, ManageEngine OpStor. To know more about how to configure ManageEngine OpStor SAN Monitoring Connector Click [here](#).

Note: By clicking on the Jump To link in the Web Client, You can shift to ManageEngine ServiceDesk Plus /ManageEngine OpManager Network Monitoring Connector / ManageEngine OpStor SAN Monitoring Connector

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.

Personalize Web Client

You can personalize the Applications Manager web client to suit your tastes. There are options to change the web client skin and layout, set the auto-refresh time for web client and customize the tabs.

Select the **Personalize Web Client** option from the 'Admin' tab. A pop-up window with 3 tabs named **Skin**, **Web Client** and **Customize Tabs** will be displayed.

To Change Web Client Skin and Layout

1. From the **Skin** tab, select the color of your choice. The colors available are blue, green, brown and orange.
2. Select the layout of your choice. The options available are **Classic** and **Simple**. The Simple layout will be similar to the Classic layout, except for the absence of links on the left hand side and the top band. The monitoring data gets more prominence in the Simple layout.
3. Click the **Apply** button. This changes the color and layout of the client's look and feel.

Auto-Refresh Web Client

Using this option, you can set the time interval for auto refreshing the web client. This option is available under the **Web Client** tab.

Customize Tabs

The default order of tabs in the Applications Manager web client is Home, Monitors, EUM, Alarms, Reports, Support and Admin. You can re-arrange the order in which the tabs are displayed as well as select new tabs for displaying. Just select the necessary tab options from the respective drop-down boxes and click the 'Save' button.

If you want to remove a tab, choose the 'Not Selected' option from the drop-down box against the necessary tab order. This option is available from the fourth tab onwards.

Integration with Portals

Applications Manager provides various options through which its monitoring data can be integrated into web portals or third-party sites. These options include:

- REST API
- JSON Feed
- Dashboards
- Google Map

REST API

Applications Manager provides REST-style APIs for fetching data from Applications Manager and integrating them into an internal portal or a third-party system management software. These data can be inserted to your own database or put in any format that you need. To start using our APIs, you need a valid Applications Manager user account and an API key.

For complete information on how to use our REST APIs, please refer this section.

JSON Feed

JSON feeds are used as an alternative for using XML for asynchronously transmitting structured information between client and server. It is a lightweight text-based open standard designed for human-readable data interchange.

Applications Manager provides the status of monitors and monitor groups in the form of JSON feeds. Using these feeds, you can integrate Applications Manager's data into your intranet web portal.

To view the status of monitors/monitor groups, access this URL:

```
<http://<Applications Manager Hostname>:<port>/jsonfeed.do?method=createMonitorGroupFeed>
```

We bundle a sample file (jsonsample.html) under <AppManager_Home>/working/html directory to parse the JSON data.

The following changes should be done in the jsonsample.html file:

- Change the hostname and port in the URL in first line in the sample file to suit your environment.

```
<script
src="http://<appmanagerhostname>:<port>/jsonfeed.do?method=createMonitorGroupFeed">
```

```
Example: <script
src="http://<appmanager>:<9090>/jsonfeed.do?method=createMonitorGroupFeed">
```

- If you want to view the monitor group status coming through JSON feed, you can invoke the URL below:

```
http://<appmanagerhost>:<port>/html/jsonsample.html
```

Dashboards

Applications Manager monitors over 50 applications and servers out-of-the-box and tracks a variety of performance indicators for each application or server monitored. In a typical IT environment however, there are certain servers and metrics that are more business critical than others. Therefore, you might want to provide more importance to those servers and their metrics. Dashboards are an easy way to put together such business-critical applications and view their performance and alerts at one place.

Applications Manager provides 4 dashboards by default - default dashboard, business view, Availability and Qos Worldwide. In addition, you can create custom dashboards such as ones that capture the status of all web applications deployed in a Tomcat server or status view of all databases and so on.

For more information on dashboards, refer this section.

World Map Business View

World Map Business View in Applications Manager enables network administrators to get a comprehensive understanding of how distributed their network really is.

You can represent a monitor group in the World Map. Monitor Groups are a logical group of one or more monitors that provides a holistic view of your business environment. You can visually represent the status of all your monitor groups across the globe. The root cause analysis (RCA) data is available in the map.

To represent **Monitor Groups** in World Map, follow the given steps.

- While creating a new monitor group, you can associate the monitor group to the location chosen from the list.
- Else, click on **Advanced** and then **Add Location**, it opens up a world map. From the map, you can select and add custom locations.

You can also save the zoom level, as per your need, by clicking on the option, “*Save current zoom level*” present in the right top corner of the web client.

World Map Settings

1. You can add or delete location from the 'Manage Location' drop down box.
2. You can click Add Location, it opens up a world map.
3. To navigate to a location, use the controls on the top left of the map.
4. Select a location in the Map by clicking it with the mouse. You will see an image indicating your selection.
5. Add a name for the location in the 'Location Name' field and click 'Add Selected Location'.
6. You can also customize the Height and Width of the World Map.

Note: To know, how to integrate Google Map in Applications Manager, click [here](#)

Reporting

The topics covered in this section are:

- Reports Settings
- Enable Reports
- Schedule Reports
- Business Hours

Reports Settings

This section explains the report settings that can be configured in Applications Manager as well as data retention settings. To access this section, click the **Report Settings** link under **Admin** tab. The section consists of the following two inner tabs:

- Reports Settings
- Data Retention
- Logo Settings

Reports Settings

Availability Reporting:

Treat Monitor Groups as Application Cluster (Availability based on default calculation) : By default, the Monitor Group availability will be shown as down (0%) if any one of the monitors in the Monitor Group is down.

Treat Monitor Groups as Services Group: By selecting this option, you can calculate Monitor Group availability based on the services availability. For eg., if there are 5 monitors in a Monitor Group and one monitor is down, Monitor Group availability is calculated as 80% available (one monitor - 20%).

Do not include Scheduled Maintenance and Unmanaged state in availability reporting: If you select this option, you can exclude scheduled maintenance and unmanaged state data from availability reports.

Attributes Reporting:

Plot attributes report with Bar chart: If you select this option, you can view the attributes report in the form of bar charts.

Plot attributes report with Line Graph: If you select this option, you can view the attributes report in the form of line graphs.

Show Plot shape in graph: By selecting this option, you can see the dots / blobs in the line graphs.

Moving Average: A simple moving average is the unweighted mean of the previous n data points. For example, a 10-day simple moving average of attribute value like CPU utilization is the mean of the previous 10 days' CPU Utilization value. By selecting this option, you can add moving average graph in the 7, 30 graphs of the various monitors.

Data 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 six hours max, 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 'Reports Settings' section, click **Data Retention** tab.
- 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 recent **alarms** that should be maintained in the alarm database.
- **Save** the changes.

Logo Settings

Click on the Logo Settings Tab to configure the report logo settings. By default, presentation reports display the ManageEngine Applications Manager 10 Logo in the upper left corner.

- Click on **Change** to change the logo.
-
- Click on the **Browse** button and select an Image.
-
- Click on **Save** to set the logo.

The user can change Logo in pdf and Excel Report. The ideal image size should be about 262*54 Dimensions and not more than 100KB. You can upload any file in format /gif/jpg/png

Enable Reports

Using this option, you can generate reports with additional performance metrics for selected resource(s)/monitor(s) apart from already available performance metrics.

To Enable Reports

1. Click on the **Admin** tab
2. Under **Applications Manager Server Setting**, click on **Enable Reports**.

Now you can configure **Custom Monitors** and **Downtime Summary Report** by following the steps given below.

Custom Monitors

1. Under **Custom Reports** tab, you will be able to select the required resource and associated performance metrics.
2. Select the tick box besides the performance metric that needs to be included in the reports.
3. Click **Save** button below and the selected performance metric will be added automatically in your reports and in your scheduled reports.

Downtime Summary Report

1. The **Downtime Summary Report** is enabled by default.
2. This option sends out a downtime summary for all resources that are monitored. The email will be sent in html format to the specified email id.
3. To configure new email action, click **New Action** and provide the email address and click **Save**.
4. This report will provide you the **top 20** downtime summary of all individual monitors.

Another method to **Enable Reports**:

1. Click on **Reports** tab
2. You can enable reports by clicking on **Enable Reports** link above the **Monitor Group**.
3. Follow the steps prescribed above to select the required attributes.
4. If email actions are already configured, select the email to which the reports need to be sent else you can configure new email action.
5. Click **Save** to create the reports schedule.

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 types, monitor groups 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.

Note: *Reportadmin* user is used to generate EmailPDF and Schedule Reports Feature. The password is generated dynamically for each and every user, hence no one can access the webclient using this username and password as this is secured.

Business Hours

Business hours is a pre-determined set of hours which helps you to view reports for the particular hours during the day. Instead of viewing data for the entire 24 hour period, you can now view reports for the particular business hour you have set. It helps you identify the critical issue which may have arisen during business hour for a particular application or resource.

To create a business hour, follow the instructions given below:

1. Click on **Admin** tab. Under **Applications Manager Server Settings** click on Business Hours icon.
2. Click on **New Business Hour** link.
3. Provide **Name** for the business hour (Eg. Office Hours). Provide **Description** for that business hour.
4. Now select which day(s) do you want to view reports for. Then select the time period for which you would like to view the reports for. Refer to the screenshot for reference:

[Admin](#) > **Business Hours**

Business Hours				
Name*	Office Hours			
Description	View reports during office hours.			
Time Settings	<input checked="" type="checkbox"/> Monday	09	00	to 18 : 30
	<input checked="" type="checkbox"/> Tuesday	09	00	to 18 : 30
	<input checked="" type="checkbox"/> Wednesday	09	00	to 18 : 30
	<input checked="" type="checkbox"/> Thursday	09	00	to 18 : 30
	<input checked="" type="checkbox"/> Friday	09	00	to 18 : 30
	<input type="checkbox"/> Saturday	00	00	to 00 : 00
	<input type="checkbox"/> Sunday	00	00	to 00 : 00
Save		Cancel		

5. Click **Save**.

Once the business hour is created, you can now generate various reports for the particular business hours you have created.

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 : *<AppManager-home>\working\mibs*.
- Scripts for execution in the *<AppManager-home>\working* or *<AppManager-home>\resources* folder and then give the path appropriately with respect to the *<AppManager-home>\working* folder.

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.

Edit Display Names:

This option enables you to bulk edit the Display Names of the Monitors.

Update Polling Interval:

This option enables you to bulk update poll intervals across monitor types.

For eg., if you have five apache servers running, you can select all the five apache servers from the list. Click on Update Polling Interval link. Your selection would be listed and you can enter the desired poll interval.

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.

Currently we do not support the copy and paste function for the following monitors.

- Custom Monitors
- Java Runtime
- php
- http URLs
- http URL Sequence
- Web Services
- Web Server
- JMX Application
- Ping Monitor
- Glassfish
- Silverstream
- MQ Series
- Office Sharepoint

Data Backup

By executing the scripts **BackupMysqIDB.bat/.sh** and **RestoreMysqIDB.bat/.sh**, you can take a backup of the data and restore it when needed.

- You will find the BackupMysqIDB.bat/.sh under *<Applications Manager Home/bin>*
- To back up data, execute the following command in command prompt
BackupMysqIDB.bat/.sh
 the output (back up data) would be put under *<working/backup/backupzip_date_time>*
 for eg.,
/<working/backup/backupzip_Jan_3_2008_14_51_15/backupzip_Jan_3_2008_14_51_15.zip>/
- To restore the backup data, Execute the following command in command prompt
RestoreMysqIDB.bat/.sh <Absolute path of the zip file that was backed up on executing BackupDB script >
 For eg., RestoreDB.bat
"C:\AppManager10\working\backup\backupzip_Jan_3_2008_14_51_15\backupzip_Jan_3_2008_14_51_15.zip"

Important: While restoring backup, Applications Manager and Applications Manager's MySQL DB should not be running.

Note: In order to backup **Web Service monitors**, after executing the BackupMysqIDB.bat/.sh take a back up of the *<AppManagerHome>/working/users/WSM* directory. To restore the same, after executing RestoreMysqIDB.bat/.sh, copy the backed up WSM directory to *<AppManagerHome>/working/users* directory

Server Settings

By editing **AMServer Properties file** & **AvailabilityTests.conf file** (AppManager Home/Conf/), you can change the default server settings used in ManageEngine Applications Manager.

AMServer Properties file	
am.webserver.port=9090	This is the web server port used by Applications Manager to connect to the browser.
am.mysql.port=13326	This port is used by Applications manager's MySQL. If this port is occupied when Applications Manager starts, it will be changed automatically.
am.tomcat.shutdown.port=18005 am.webcontainer.port=18009 am.rmiregistry.port=11099 am.shutdown.port=12000	Tomcat ports for Applications Manager. If any of these ports is occupied when Applications Manager starts, it will be changed automatically.
# specify whether these ports need to be checked or not. am.mysqlport.check=true am.webserverport.check=true	Once Applications Manager starts, it will check if it can access the MySQL port & Web Server port. If it cannot access the port, it will assume that you are unable to start the service and it will shut down Applications Manager. To disable this test, you have to change these values.
#Start up the browser when the server starts up. am.browser.startup=true	In windows, the browser will automatically open when Applications Manager starts. Change the following to false if you do not want the browser to open automatically.
am.upload.enabled=true	If you do not want to enable file uploads using Admin tab -> Upload Files/Binaries, change the option to false.
am.cam.mbeanslistsize=250	While adding custom attributes in JMX /JBoss / Weblogic / WebSphere monitors, only 250 MBeans will be listed by default. If you want more number of MBeans to be listed, change the number. This has been done to reduce the page loading time and over head on Applications Manager Server.
#am.pingtest.command=/bin/ping -c 1 -w 1	Applications Manager executes the ping command to check the availability of a server. You can change the ping command if the options mentioned are not working.

am.server.type=N.A am.adminserver.host=N.A am.adminserver.port=N.A am.server.startresidrange=N.A	These entries will be used in Enterprise Edition of ManageEngine Applications Manager.
am.filesize.unit=KB (bytes,MB,GB) am.dirsize.unit=MB (bytes,KB,GB)	Default units of File Size and Directory Size (File system Monitoring) is in KB & MB. You can alternatively use bytes, MB or GB.
#Valid options for language and country en/US,zh/CN,ja/JP, vi/VN am.server.language=en am.server.country=US	These options are used to change Applications Manager's language to Japanese (ja / jp), Chinese (zh / CN) or Vietnamese (vi / VN).
AvailabilityTests.conf file	
am.porttestenabled=false am.portstotest=80,21	In Applications Manager, the availability of the system is checked by using ping test. If the ping test fails, it is said that the system is down. If ping is disabled in your environment or if you want additional tests to be performed in addition to the ping test , enable the am.porttestenabled option. If this option is enabled, in addition to performing ping test, Applications Manager will check if you are able to access the ports mentioned in am.portstotest in the machine which you are trying to monitor. You can specify multiple ports in the am.portstotest separated by commas. If you are able to access any one port, system is not said to be down. This option can be used to reduce false alarms / when ping command is not present in the Applications Manager machine.
am.porttest.timeout.seconds=5	This value is the time out value used in Applications Manager for checking all monitors.
am.ping.retries=0	The number of times the ping command should try again before stopping.
am.enablenativeping=false	If you change the below option as true, then start Applications Manager as root in linux and admin user in Windows, this option is to enable the native ping test (if native ping is enabled, native ping will also be tested in addition to normal ICMP ping).
am.tomcattimeout=5	This option is to set timeout level for tomcat version 5

Production Environment

This document covers configuration details that you need to take care of when moving Applications Manager into Production:

User Accounts (OS User / Applications Manager Web Client User)

Note: OS User will be referred to as *OS User*. A user login account to the Applications Manager Web Client will be referred to as *Web Client User*. Refer User Administration document for more information on users.

- Make sure you change the password for the default "admin" Web Client User within Applications Manager.
- Have a dedicated OS User (System) account for installing Applications Manager. This OS user account needs full permissions on all folders and sub-folders in the installation root of Applications Manager only. Also make sure this OS User account is fully secure. It is NOT necessary to install Applications Manager in a root (in Linux) or administrator (windows) OS User account. But make sure the whole installation is done using the same OS user account. Do not install using root and try to run using an OS user account. That will fail.
- If you want to give full "Read-Only" privileges to certain Web Client Users in your organisation, then make sure you create a client login with "USER" role.
- If you want to give restricted "Read-Only" privileges to certain Web Client Users in your organisation, then make sure you create a client login with "Operator" role. "Operator" can view only servers that they own.
- **Note:** Access to the default MySQL database is restricted to the installation host alone by default. It is recommended to change the default password.

To change MySQL Database password, follow the below given steps:

1. Connect to Applications Manager's MySQL. Go to *<AppManager10/working/MySQL>*, execute the following command

```
./bin/mysql -u root -h localhost --port=13326 -D AMDB -pappmanager
```

2. Execute the following queries in the database

```
USE mysql
```

```
update user set password=password ('New Password') where user = 'root'
```

```
FLUSH PRIVILEGES;
```

3. Then stop Applications Manager.

4. Go to `<AppManager10/working/conf>` folder, edit `<databaseparams.conf>` and change the password to the 'New' password. Restart Applications Manager.

Other General Guidelines

- Refer the Security/Firewall Requirements document to understand what changes are required in the firewall.
- You can install Applications Manager as a Windows Service or configure a cron job on Linux to start on server start up.
- If you are planning to use the Enterprise Edition, fully understand the EE architecture.
- By default, uploading binaries, MIBs, scripts are allowed in Applications Manager. This may be required in the initial stages while using Applications Manager for uploading MIBs, action scripts etc. However while going in to production, it is strongly recommended to disable this.
- Are you getting false alarms for server availability? This could be because, your production servers are taking too long to respond. You can set higher timeouts.
- To change the default HTTP port used by Applications Manager, refer the Server Settings document. You can refer to this document on other settings that you can modify. For eg., whenever Applications Manager starts, if you do not want the browser to open automatically, you need to modify the entry `<am.browser.startup=false>`
- Backup the Applications Manager configuration and data.

From a **security point of view**, the following are done :

- All passwords are encrypted
- The encryption keys are uniquely generated for each customer environment.

Note: Kindly inform appmanager-support@manageengine.com, if you feel that some more information can be added.

REST APIs

Applications Manager REST APIs

ManageEngine Applications Manager provides REST APIs for fetching data from Applications Manager. Using these APIs, Applications Manager's data can be integrated with any internal portal or 3rd party System Management software. The data can be represented in a single dashboard itself.

By using any XML parser in a scripting language, Java, C, Perl or Python, etc. you can make HTTPs requests in the format recommended in the API. This data can then be inserted into your own database or put in any format that you need.

Prerequisites

Applications Manager User Account

Each Applications Manager User should have a valid UserName to use the API.

Take an intranet portal for example. When each user logs in, the assigned monitors and alarms will be shown. So, it is imperative that each user should have separate API keys. When GetAlarms API is invoked with the key generated for that particular operator, it will list the alarms that are assigned to that person alone.

How do APIs work?

In order to use the API, each user should obtain an API key - which is a long text and is unique to their Applications Manager Account. The API key has to be passed as parameter in every API request made.

Generate API Key

The User can register for the API key from within Applications Manager product using the "REST API" option in the Admin tab.

Note: Generating the API key is a one-time process.

Steps for using REST API

- Click on the **Admin** tab
- Under Applications Manager Server Settings, click on **REST API**.

- The API key is generated - eg. 7b5fde68148fa2419bc2f1a1ab87e757
- Open the browser, the URL would be
http://<myappmanager-server>:9090/AppManager/xml/ListServer?apikey=7b5fde68148fa2419bc2f1a1ab87e757&type=all
- By changing <type> to the required monitor, data pertaining to that monitor can be retrieved.
Check if the following URL works fine
http://<myappmanager-server>:9090/AppManager/xml/ListServer?apikey=7b5fde68148fa2419bc2f1a1ab87e757&type=server
will give data of all the server monitors. 'all' will give the entire Applications Manager's data.
- By using any xml parser in a scripting language, Java, C, Perl or Python etc, you can make HTTPs requests in the format recommended in the API. This data can then be inserted into your own database or put in any format that you need.

API Description

REST Command	Description	XSD
ListMonitor	This API allows the user to know the availability, health status of monitors, type, state - managed/unmanaged, etc.	ListMonitor.xsd
ListServer	This API allows the user to know the details of servers like IP Address, status, services running in them, etc.	ListServer.xsd
ListAlarms	This API allows the user to know the details like alarm state - critical/warning/clear, type, top N alarms, time bound alarms, etc.	ListAlarms.xsd
Manage / UnManage	This API allows the user to Manage or UnManage a Monitor in Applications Manager by using ResourceID.	ManageMonitor.xsd UnmanageMonitor.xsd
CreateMaintenanceTask	This API allows the user to create a downtime schedule.	CreateMaintenanceTask.xsd
EditMaintenanceTask	This API allows the user to edit a downtime schedule.	EditMaintenanceTask.xsd

REST Command	Description	XSD
DeleteMaintenanceTask	This API allows the user to delete a downtime schedule.	DeleteMaintenanceTask.xsd
GetMonitorData/ListMonitorData	This API allows the user to fetch data of the latest poll from monitors.	ListMonitorData.xsd
AddMonitor	This API allows the user to the user to add monitors in Applications Manager.	AddMonitor.xsd
ListMaintenanceTaskDetails	This API allows the user to list all the scheduled downtime.	ListMaintenanceTaskDetails.xsd
AddMonitorGroup	This API allows the user to add a new Monitor Group.	AddMonitorGroup.xsd
PollNow	This API allows the user to poll a monitor.	PollNow.xsd
DeleteMonitor	This API allows the user to delete the monitor.	DeleteMonitor.xsd

Note: You can obtain the resourceid of a monitor by executing the ListMonitor API request. The output of this request contains resourceid of the monitor, among other values.

REST API xsd files are available in AppManager10/help/RESTAPI/xsd folder.

List Monitor API

ManageEngine Applications Manager provides List Monitor API that allows the user to list details of monitor by the following categories.

- By monitor Type
- By monitor ResourceID
- Listing all the added monitors

APIs for ListMonitor

1. By monitor Type

http://[Host]:[Port]/AppManager/xml/ListMonitor?apikey=[API key]&type=[TYPE in AM_ManagedObject table]

2. By particular monitor name

http://[Host]:[Port]/AppManager/xml/ListMonitor?apikey=[API key]&resourceid=[Resourceid]

3. Listing all the added monitors

http://[Host]:[Port]/AppManager/xml/ListMonitor?apikey=[API key]&type=all

Request Parameters

Field	Description
API Key	The key generated from "Generate API" option in the Admin tab.
Type	"type=<monitor type>" is used to list all the monitors in a specified monitor type. <monitor type> is TYPE in AM_ManagedObject table like Linux, Windows XP, MYSQL-DB-server, Apache-server, UrlMonitor, Tomcat-server, etc.
resourceid	The resourceid of the monitor

Example API that is used to get XML of monitors by monitor type.

http://app-windows:9090/AppManager/xml/ListMonitor?apikey=[Api Key]&type=[Type]

Example API that is used to get XML of all monitors.

http://app-windows:9090/AppManager/xml/ListMonitor?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8

Example API that is used to get XML of a particular monitors.

`http://app-`

`windows:9090/AppManager/xml/ListMonitor?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&resourceID=10000047`

Example output:

Monitor Details:

DISPLAYNAME	Monitor's Display Name
RESOURCE ID	Monitor's Resource ID
TYPE	Monitor type like Windows, Linux
Health Details	Contains HEALTHMESSAGE that gives the Health Root Cause Message, Health Attribute ID, HEALTHSEVERITY - (5/4/1) - Clear/Warning/Critical , STATUS - Clear/Warning/Critical
Availability Details	Contains AVAILABILITYMESSAGE that gives the Availability Root Cause Message, Availability Attribute ID, AVAILABILITYSEVERITY - Up/Down (5/1), STATUS - UP/Down
Managed	True - the monitor is in Managed state, False - the monitor is in Unmanaged State
RESOURCENAME	Monitor's Resource Name
DESCRIPTION	Description of the Resource like Network Resource
RCAPageURL	URL that links to Root Cause Analysis details
DetailsPageURL	URL that links to details page of the monitor

```
<AppManager-response uri="/AppManager/xml/ListMonitor">
  <result>
    <response response-code="4000">
      <Monitor DISPLAYNAME="myes" RESOURCEID="10000025" TYPE="Windows XP" RESOURCENAME="myes"
DESCRIPTION="Network Resource" Managed="true"
DetailsPageURL="showresource.do?resourceid=10000025&method=showResourceForResourceID&PRINTER_FRIENDLY=true"
RCAPageURL="jsp/RCA.jsp?resourceid=10000025&attributeid=1651" HEALTHATTRIBUTEID="1651"
HEALTHMESSAGE="Health of myes is clear. <br>Root Cause : <br>1. myes is up<br>" HEALTHSEVERITY="5"
HEALTHSTATUS="clear" AVAILABILITYATTRIBUTEID="1650" AVAILABILITYMESSAGE="Resource up. <br>The
resource myesuraj.zohocorpin.com is available." AVAILABILITYSEVERITY="5" AVAILABILITYSTATUS="up"/>
    </response>
  </result>
</AppManager-response>
```

List Server API

ManageEngine Applications Manager provides List Server API that allows the user to list information about the server by the following categories.

- Listing all the server details.
- By particular server name.
- By IP Address of server.

APIs for ListServer:

1. Listing all the added servers

http://[Host]:[Port]/AppManager/xml/ListServer?apikey=[API key]&type=all

2. By server name

http://[Host]:[Port]/AppManager/xml/ListServer?apikey=[API key]&type=[Server display name]

3. By IP Address

http://[Host]:[Port]/AppManager/xml/ListServer?apikey=[API key]&ipaddress=[IP Address of server]

Request Parameters

Field	Description
API Key	The key generated from "Generate API " option in the Admin tab.
Type	"type=<Server PARENTNODE name>" is used to list details of specified server in Applications Manager < Server PARENTNODE name> is PARENTNODE in IpAddress table.
ipaddress	ipaddress = [IP Address of server]

Example API that is used to get the XML of all servers and their services details

http://app-windows:9090/AppManager/xml/ListServer?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&type=all

Example API that is used to get XML of a particular server and its services details.

<http://app-windows:9090/AppManager/xml/ListServer?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&type=app-windows>

Example output:**Server Details:**

Server Name	Name of the Server
Parent IP	Parent Network IP address of the Server
resourceid	Resource ID of the Server
Type	Server Type like Windows
DISPLAYNAME	Display Name of the Server like XP1
IPADDRESS	IP Address of the Server
Service Details	Contains information about the services running in the server. Service DISPLAYNAME - Display Name of the Service TYPE - Type of the service like SNMP RESOURCEID - Resource ID of the Service RESOURCENAME - Resource Name of the Service DESCRIPTION - Description of the Resource like Network Resource ATTRIBUTEID - Service Attribute ID
RCALink	Link to Root Cause Analysis details
DetailsPageLink	Link to the Details page of the Server

```
<AppManager-response uri="/AppManager/xml/ListServer">
  <result>
    <response response-code="4000">
      <Server Name="app-xp1.zohocorpin.com" PARENTIP="192.168.110.0" RESOURCEID="10000070"
TYPE="Windows XP" DISPLAYNAME="XP1" IPADDRESS="192.168.110.234">
<Service DISPLAYNAME="app-xp1.zohocorpin.com_SNMP_161" TYPE="SNMP" RESOURCEID="10000322"
RESOURCENAME="IF-app-xp1.zohocorpin.com_SNMP_161" DESCRIPTION="Network Resource"
ATTRIBUTEID="1750" DetailsPageLink="/showresource.do?resourceid=10000322&method=showResourceForResourceID"
RCALink="/jsp/RCA.jsp?resourceid=10000322&attributeid=1750"/>
</Server>
    </response>
  </result>
</AppManager-response>
```

List Alarms API

ManageEngine Applications Manager provides List Alarms API that allows the user to list the information regarding recent alarms in an XML format. The alarm APIs are listed as follows.

- Listing all recent alarms
- Listing all critical recent alarms
- Listing all warning recent alarms
- Listing all clear recent alarms
- Listing recent alarms by time filter
- Listing alarms by monitor type
- Listing alarms by monitor resourceid
- Listing alarms by top N

APIs for ListAlarms.

- Listing all the alarms.

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]

- Listing all critical recent alarms

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&type=critical

- Listing all warning recent alarms

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&type=warning

- Listing all clear recent alarms

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&type=clear

- Listing recent alarms after specified time.

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&time=[Time]

- Listing alarms by monitor name

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&resourceid=[resourceid]

- Listing alarms by monitor type

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&type=[TYPE]

- Listing alarms by top N

http://[Host]:[Port]/AppManager/xml/ListAlarms?apikey=[API key]&topN=[N]

Request Parameters

Field	Description
API Key	The key generated from "Generate API" option in the Admin tab.
resourceid	"resourceid=[resourceid of monitor]" is used to list the alarms of particular monitor.
Type	

Field	Description
	<p>"type=all" is used to list all alarms.</p> <p>"type=critical" is used to list all the critical alarms.</p> <p>"type=warning" is used to list all the warning alarms.</p> <p>"type=clear" is used to list all the clear alarms.</p> <p>"type=[Monitor type]" is used to list alarms by monitor type where <monitor type> is TYPE in AM_ManagedObject table like Linux, Windows XP, MYSQL-DB-server, Apache-server, UrlMonitor, Tomcat-server, etc.</p>
Top N	"topN=[N]" is used to list the top N alarms.
Time	<p>"time=[Time]" is used to list the alarms generated after the specified time.</p> <p><Time> is represented in milli second.</p>

Example API that is used to get XML of all recent alarms details.

<http://app-windows:9090/AppManager/xml/ListAlarms?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a>

Example output:

Alarm Details

DISPLAYNAME	Display Name of the Monitor like Linux-1
RESOURCEID	Resource ID of the Monitor
SEVERITY	Clear/Warning/Critical - (5/4/1)
MESSAGE	Alarm message like 'Resource is down. Health is critical as the resource is not available'
ATTRIBUTE ID	Attribute ID of health of monitor
MODTIME	Time when the Alarm was generated (ms)
STATUS	Clear/Warning/Critical - status of the alarm
TYPE	Type of the Monitor like Linux
TYPEDISPLAYNAME	Display Name of the Type like 'Linux'

```

<AppManager-response uri="/AppManager/xml/ListAlarms">
  <result>
    <response response-code="4000">
      <Alarm RESOURCEID="10000112" DISPLAYNAME="Linux1" TYPE="Linux" TYPEDISPLAYNAME="Linux"
SEVERITY="1" STATUS="critical " MESSAGE="Health of Linux1 is critical. <br>Root Cause : <br>1. Total Disk
Utilization(%) 54.0 > 52.0 (Anomaly).<br><br>" ATTRIBUTEID="701" MODTIME="1263361294086"/>
    </response>
  </result>
</AppManager-response>

```

Example API that is used to get XML of all recent alarms details which are generated after a particular time.

http://app-
windows:9090/AppManager/xml/ListAlarms?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&time=124
8868798412

Manage API

ManageEngine Applications Manager provides Manage API that allows the user to manage a monitor. More..

UnManage API

ManageEngine Applications Manager provides UnManage API that allows the user to unmanage a monitor. More..

API to Manage a Monitor

http://[Host]:[Port]/AppManager/xml/ManageMonitor?apikey=[API key]&resourceid=[RESOURCEID]

Note: This API is not supported for Admin Server.

Request Parameters

Field	Description
API Key	The key generated from "Generate API Key" option in the Admin tab.
resourceid	resourceid=[RESOURCEID] where RESOURCEID is the AM_ManagedObject.RESOURCEID of the monitor to be managed.

The following is an example for ManageMonitor

http://app-windows:9090/AppManager/xml/ManageMonitor?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&resourceid=10000031

Example output:

```
<AppManager-response uri="/AppManager/xml/ManageMonitor">
  <result>
    <response response-code="4000">
      <message>Monitor with resourceID 10000031 managed successfully</message>
    </response>
  </result>
</AppManager-response>
```

API to UnManage a Monitor

http://[Host]:[Port]/AppManager/xml/UnmanageMonitor?apikey=[API key]&resourceid=[RESOURCEID]

Request Parameters

Field	Description
API Key	The key generated from "Generate API Key" option in the Admin tab.
resourceid	resourceid=[RESOURCEID] where RESOURCEID is the AM_ManagedObject.RESOURCEID of the monitor to be unmanaged.

The following is an example for UnManageMonitor

http://app-windows:9090/AppManager/xml/UnmanageMonitor?apikey=65d0fa3e1f6c6bdcce1c3969f24c39a8&resourceid=10

Example output:

```
<AppManager-response uri="/AppManager/xml/UnmanageMonitor">
  <result>
    <response response-code="4000">
      <message>Monitor with resourceID 10 unmanaged successfully</message>
    </response>
  </result>
</AppManager-response>
```

Authenticator API

For mobile applications, new users may need to reuse the API Key provided to successfully authenticated users, so that they can use it for remaining operations. Authenticator API allows users to fetch details like the their API Keys, Roles, image and any other information associated to the user for successful authentication.

NOTE:

We hope to make it available only in HTTPS (SSL) Mode & POST Method.

API for XML Response : [http://\[APM Host \]:\[APM Port \]/AppManager/xml/Authenticator](http://[APM Host]:[APM Port]/AppManager/xml/Authenticator)

API for JSON Response : [http://\[APM Host \]:\[APM Port \]/AppManager/json/Authenticator](http://[APM Host]:[APM Port]/AppManager/json/Authenticator)

Request Parameters:

Field	Description
j_username	Username has to be posted to the above mentioned request with 'j_username' as parameter name.
j_password	Password has to be posted to the above mentioned request with 'j_password' as parameter name.

Request Parameters:

a) j_username: Username has to be posted to the above mentioned request with 'j_username' as parameter name.

b) j_password: Password has to be posted to the above mentioned request with 'j_password' as parameter name.

Response Details:

Field	Description
APIKey	This is the username.
Description	This is the description of the user account given at the time of creation of user account
EmailID	This is the e-mail id of the user
GroupName	This is the typ of account the user has. ex: operator, admin, manager etc.
UserImage	This is User image path

Field	Description
UserID	This is the ID of the user
UserName	This is the username of the user.

```
<AppManager-response uri="/AppManager/xml/Authenticator">
<result>
<response response-code="4000">
<UserDetails EmailID="NA" UserID="1" Description="NA" UserName="admin"
APIKey="8c8ec3f2cd30722d3a6f980df12c1e5f" UserImage="/images/icon_user.gif"
GroupName="ADMIN"/>
</response>
</result>
</AppManager-response>
```

ExecuteAction

This API will be used to execute the actions that are configured in Applications Manager. An Operator can only execute an action that is associated to him.

API for XML Response:

```
http://[ APM Host ]:[ APM Port ]/AppManager/xml/ExecuteAction?apikey=[ API Key
]&ActionId=10000056
```

API for JSON Response:

```
http://[ APM Host ]:[ APM Port ]/AppManager/json/ExecuteAction?apikey=[ API Key
]&ActionId=10000056
```

Request Parameters:

Field	Description
ActionId	This value specifies the action id and helps the API to execute the corresponding action.

```
<AppManager-response uri="/AppManager/xml/ExecuteAction">
<result>
<response response-code="4000">
<ExecuteAction ActionTypeID="2" Status="Success"
ActionExecPath="/common/executeSMS.do?method=testAction&actionID=10000004" Message="The
action test1 has been successfully executed" ActionName="test1" ActionID="10000004"
ActionType="SMS Action(s)"/>
</response>
</result>
</AppManager-response>
```

NOTE: For the Actions like Ec2Instance / VMActions / Service actions (Start/ Stop/ Restart) will execute the action directly. where as in UI we are asking the user to send a test mail or to execute the action.

ListDashboards API

This API fetches the List of Dashboards created in the Server which includes all the widgets configured in the Dashboards as there is no concept of assigning the dashboards/widgets to operators. But the data which is to be populated will be based on the monitors assigned for the user.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListDashboards?apikey=[Api Key]`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListDashboards?apikey=[API Key]`

Response Details:

Field	Description
DashboardId	This is the username.
DashboardName	This is the description of the user account given at the time of creation of user account
Widget	WidgetName -- This represents the display name of the widget WidgetId -- This is the id of the widget created in this dashboard. WidgetURL -- This is the link to the widget of this dashboard

```
<AppManager-response uri="/AppManager/xml/ListDashboards">
<result>
<response response-code="4000">
<Dashboard DashboardId="10000001" DashboardName="Default Dashboard">
<Widget WidgetName="Top N Monitors" WidgetId="10000040"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000040"/>
<Widget WidgetName="Current Availability " WidgetId="10000044"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000044"/>
<Widget WidgetName="Last 24 Hours / 30 Days Availability History" WidgetId="10000046"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000046"/>
<Widget WidgetName="Last 24 Hours / 30 Days Health History" WidgetId="10000047"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000047"/>
<Widget WidgetName="Availability,Health and Alarm Summary" WidgetId="10000048"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000048"/>
<Widget WidgetName="Monitor Groups" WidgetId="10000057"
```

```
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000057"/>
<Widget WidgetName="Infrastructure Snapshot" WidgetId="10000078"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000078"/>
<Widget WidgetName="Recent 10 Alarms" WidgetId="10000079"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000079"/>
<Widget WidgetName="Performance Metric Widget" WidgetId="10000088"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000001&widgetid=10000088"/>
</Dashboard>
<Dashboard DashboardId="10000005" DashboardName="pavan dashboard">
<Widget WidgetName="Top N Monitors" WidgetId="10000007"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000005&widgetid=10000007"/>
<Widget WidgetName="Tabular Data" WidgetId="10000008"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000005&widgetid=10000008"/>
<Widget WidgetName="Recent 10 Alarms" WidgetId="10000009"
WidgetURL="/MyPage.do?method=getWidget&pageid=10000005&widgetid=10000009"/>
</Dashboard>
</response>
</result>
</AppManager-response>
```

ListMonitorTypes API

This API will list all the monitor types configured in the Applications Manager for the user corresponding to the API Key. The details include the Health and Availability of the monitor types, type image, Health outages, Critical/Warning/Clear/UP/Down count for each and every monitor type.

API for XML Response:

[http://\[APM Host \]:\[APM Port \]/AppManager/xml/ListMonitorTypes?apikey=\[API Key \]&type=all](http://[APM Host]:[APM Port]/AppManager/xml/ListMonitorTypes?apikey=[API Key]&type=all)

API for JSON Response:

[http://\[APM Host \]:\[APM Port \]/AppManager/json/ListMonitorTypes?apikey=\[API Key \]&type=all](http://[APM Host]:[APM Port]/AppManager/json/ListMonitorTypes?apikey=[API Key]&type=all)

NOTE:

We hope to support the others in future, depending on popular customer demand.

Response Details:

Field	Description
AVAILUNKNOWNCOUNT	This is the count of number of monitors for which availability is unknown.
IMAGE	This is the image path for the monitor type
CRITICALCOUNT	This is the count of number of monitors for which health is critical in a type
SUBGROUP \ RESCATEGORY	This represent the category under which it belongs to. (IIS-Server, Mail-Server, etc.,)
DOWNCOUNT	This is the count of number of monitors for which availability is down in a type
HEALTHSEVERITY	This is the severity of the health (1-critical, 4-warning and 5-clear)
HEALTHMSG	This is the health message for this monitor type
RESCATEGORY	This represents the group under which this monitor type is grouped. like (servers, Databases, etc.,)

Field	Description
UPCOUNT	This is the count of number of monitors for which availability is up in a type
CLEARCOUNT	This is the count of number of monitors for which health is clear in a type
OUTAGES	This is the health outages w.r.t the total number of monitors in this type
DISPLAYNAME	This is the displayname of the monitor type
WARNINGCOUNT	This is the count of number of monitors for which health is warning in a type
AVAILMSG	This is the availability message for this monitor type
COUNT	This is the total number of monitors in this type
HEALTHUNKNOWNCOUNT	This is the count of number of monitors for which health is unknown in a type
RESOURCEURL	This is the url of the page where all the monitor's of this type will be listed.
AVAILSEVERITY	This is the severity of the availability for this type (clear -5, down -1)

```
<AppManager-response uri="/AppManager/json/ListMonitorTypes">
<result>
<response response-code="4000">
<MonitorType AVAILUNKNOWNCOUNT="0" IMAGE="/images/icon_monitors_solaris.gif"
CRITICALCOUNT="0" SUBGROUP="Sun Solaris" DOWNCOUNT="0" HEALTHSEVERITY="5"
HEALTHMSG="Health is clear.<br>Root Cause:<br>1. Health of Sunsolaris is clear <br>"
RESCATEGORY="SYS" UPCOUNT="1" CLEARCOUNT="1" OUTAGES="0/1" DISPLAYNAME="Sun
Solaris" WARNINGCOUNT="0" AVAILMSG="Resource is up.<br>Root Cause:<br>1. Sunsolaris is up
<br> <br>" COUNT="1" HEALTHUNKNOWNCOUNT="0"
RESOURCEURL="/showresource.do?method=showResourceTypes&direct=true&network=Sun
Solaris&detailspage=true&PRINTER_FRIENDLY=true" AVAILSEVERITY="5"/>
<MonitorType AVAILUNKNOWNCOUNT="0" IMAGE="/images/icon_monitor_vmware.gif"
CRITICALCOUNT="7" SUBGROUP="VirtualMachine" DOWNCOUNT="8" HEALTHSEVERITY="1"
HEALTHMSG="Health is critical.<br>Root Cause:<br>1. Health of amp-vm-centos64 is critical <br>2.
```

```

Health of opman-xp32-2-test is critical <br>3. Health of opman-ubuntu10-1-ttt11 is critical <br>4.
Health of tes-111-5689-linux-2 is critical <br>5. Health of opman-ubuntu10-6-test2 is critical <br>6.
Health of Jim Linux Box is critical <br>7. Health of ICONVM is critical <br>" RESCATEGORY="VIR"
UPCOUNT="8" CLEARCOUNT="8" OUTAGES="7/16" DISPLAYNAME="Virtual Machine"
WARNINGCOUNT="0" AVAILMSG="Resource is down.<br>Root Cause:<br>1. amp-vm-centos64 is
down <br> <br>2. null is down <br> <br>3. opman-xp32-2-test is down <br> <br>4. opman-ubuntu10-
1-ttt11 is down <br> <br>5. tes-111-5689-linux-2 is down <br> <br>6. opman-ubuntu10-6-test2 is
down <br> <br>7. Jim Linux Box is down <br> <br>8. ICONVM is down <br> <br>" COUNT="16"
HEALTHUNKNOWNCOUNT="1"
RESOURCETYPEURL="/showresource.do?method=showResourceTypes&direct=true&network=VirtualMachine&detailspage=true&PRINTER_FRIENDLY=true" AVAILSEVERITY="1"/>
<MonitorType AVAILUNKNOWNCOUNT="0" IMAGE="/images/icon_monitor_SSL.gif"
CRITICALCOUNT="0" SUBGROUP="SSLCertificateMonitor" DOWNCOUNT="0"
HEALTHSEVERITY="5" HEALTHMSG="Health is clear.<br>Root Cause:<br>1. Health of ZOHO is
clear <br>" RESCATEGORY="URL" UPCOUNT="1" CLEARCOUNT="1" OUTAGES="0/1"
DISPLAYNAME="SSL Certificate Monitor" WARNINGCOUNT="0" AVAILMSG="Resource is
up.<br>Root Cause:<br>1. ZOHO is up <br> <br>" COUNT="1" HEALTHUNKNOWNCOUNT="0"
RESOURCETYPEURL="/showresource.do?method=showResourceTypes&direct=true&network=SSLCertificateMonitor&detailspage=true&PRINTER_FRIENDLY=true" AVAILSEVERITY="5"/>
</response>
</result>
</AppManager-response>

```

ListMonitorGroups API

This API will fetch all the List of Monitor Groups created in the Server which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

[http://\[APM Host \]:\[APM Port \]/AppManager/xml/ListMonitorGroups?apikey=\[API Key \]&type=all](http://[APM Host]:[APM Port]/AppManager/xml/ListMonitorGroups?apikey=[API Key]&type=all)

API for JSON Response:

[http://\[APM Host \]:\[APM Port \]/AppManager/json/ListMonitorGroups?apikey=\[API Key \]&groupId=10000035](http://[APM Host]:[APM Port]/AppManager/json/ListMonitorGroups?apikey=[API Key]&groupId=10000035)

Request Parameters:

Field	Description
type	To get all monitor groups we need to pass 'all' as the value for the field type.
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
DetailsPageURL	This is the url for the details page of the monitor group
TODAYUNAVAILPERCENT	This value represents the today's unavailability perecentage
AvailabilityRCAURL	This represents the Availability RCA Url.
Action	This represents status of the monitor group whether actions or enabled or not

Field	Description
CRITICALCOUNT	This represents the critical monitors/monitorgroups count
NAME \ DISPLAYNAME	This Represents the displayname of the monitor group
DOWNCOUNT	This represents the total number of monitors/monitor groups down in this group
TODAYAVAILPERCENT	This value represents the today's availability perecentage
TODAYSCHEDDOWNPERCENT	This value represents the today's scheduled downtime perecentage
Type	This value represents type i.e Monitor group or sub group
HEALTHSEVERITY	This represents the severity of the health for this Monitor group (1-critical, 4-warning & 5-clear)
HealthUnknownCount	This represents the number of monitors or subgroups for which the health is unknown.
AVAILABILITYSEVERITY	This represents the severity of the availability for this monitor group (1-down , 5-up)
AVAILABILITYMESSAGE	This is the availability message for this group
RESOURCEID	This is the resourceid of the monitor group.
CLEARCOUNT	This represents the number of monitors or subgroups for which the health is clear.
UPCOUNT	This represents the number of monitors or subgroups for which the availability is up.
HealthRCAURL	This represents the link which show the Health RCA of this group.
TODAYUNMANGDPERCENT	This value represents the today's unmanaged perecentage
HEALTHMESSAGE	This is the health message for this group
AvailabilityUnknownCount	This represents the number of monitors or subgroups for which

Field	Description
	the availability is unknown.
OUTAGES	This represents the number of monitors or subgroups for which the health is not clear.
WARNINGCOUNT	This represents the number of monitors or subgroups for which the health is warning.
HEALTHSTATUS	This represents health status of this group (CRITICAL / CLEAR / WARNING)
AVAILABILITYSTATUS	This represents availability status of this group (UP/ DOWN)
SubMonitorGroup	<p>DetailsPageURL --- This is the details page of the sub group</p> <p>TODAYUNAVAILPERCENT --- this is today's unavailability percentage for sub group</p> <p>AvailabilityRCAURL --- this represents the availability RCA url for sub group</p> <p>Action --- this states whether the actions are enabled for this subgroup or not.</p> <p>NAME \ DISPALYNAME --- this is the displayname of the subgroup</p> <p>TODAYAVAILPERCENT --- this is today's availability percentage for sub group</p> <p>TODAYSCHEDDOWNPERCENT --- this is today's scheduled downtime percentage for sub group</p> <p>HEALTHSEVERITY --- this is health severity of the sub group</p> <p>TYPE --- this represents whether it is subgroup/group</p> <p>AVAILABILITYSEVERITY --- this is availability severity of the sub group</p> <p>AVAILABILITYMESSAGE --- this is availability message of the sub group</p> <p>RESOURCEID --- this is resource id the sub group</p> <p>HealthRCAURL --- this is health RCA url of this sub group</p> <p>TODAYUNMANGDPERCENT --- this is today's unmanaged percentage of the sub group</p> <p>HEALTHMESSAGE --- this is health message of the sub group</p> <p>HEALTHSTATUS --- this is health status of the sub group</p> <p>AVAILABILITYSTATUS --- this is availability status of the sub</p>

Field	Description
	group

```

<AppManager-response uri="/AppManager/xml/ListMonitorGroups">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000036&
method=showApplication"
TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000036&attributeid=17" Action="enabled"
CRITICALCOUNT="0" NAME="Applications Manager"
DOWNCOUNT="0" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
Type="Monitor Group" HEALTHSEVERITY="5" HealthUnknownCount="0"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000036" CLEARCOUNT="5"
UPCOUNT="5"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000036&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is clear.
<br>Root Cause : <br>Health is Clear"
AvailabilityUnknownCount="0" OUTAGES="0/5" DISPLAYNAME="Applications Manager_karthi-0031"
WARNINGCOUNT="0" HEALTHSTATUS="clear" AVAILABILITYSTATUS="up" />
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this monitor group

Field	Description
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	<p>DetailsPageURL -----> this is details page of the sub group</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the sub group</p> <p>Action -----> this is action status of the sub group</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the sub group</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group</p> <p>HEALTHSEVERITY -----> this is health severity of the sub group</p> <p>TYPE -----> this represents the type of the group</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the sub group</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p>

Field	Description
	<p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>

```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqllexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqllexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqllexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqllexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqllexpress"

```

```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```

```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```

```

NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this

Field	Description
	monitor group
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	DetailsPageURL -----> this is details page of the sub group TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group AvailabilityRCAURL -----> this is availability RCA url of the sub group Action -----> this is action status of the sub group NAME \ DISPLAYNAME -----> this is displayname of the sub group TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group HEALTHSEVERITY -----> this is health severity of the sub group TYPE -----> this represents the type of the group AVAILABILITYSEVERITY -----> this is availability severity of the sub group AVAILABILITYMESSAGE -----> this is availability message of

Field	Description
	<p>the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p> <p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>


```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li></ol></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqlexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqlexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqlexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqlexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqlexpress"

```

```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```

```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```

```

NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group

Field	Description
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this monitor group
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	DetailsPageURL -----> this is details page of the sub group TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group AvailabilityRCAURL -----> this is availability RCA url of the sub group Action -----> this is action status of the sub group NAME \ DISPLAYNAME -----> this is displayname of the sub group TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group HEALTHSEVERITY -----> this is health severity of the sub group TYPE -----> this represents the type of the group AVAILABILITYSEVERITY -----> this is availability severity of the sub group

Field	Description
	<p>AVAILABILITYMESSAGE -----> this is availability message of the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p> <p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>


```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqlexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqlexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqlexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqlexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqlexpress"

```



```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```

```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```

```

NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group

Field	Description
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this monitor group
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	DetailsPageURL -----> this is details page of the sub group TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group AvailabilityRCAURL -----> this is availability RCA url of the sub group Action -----> this is action status of the sub group NAME \ DISPLAYNAME -----> this is displayname of the sub group TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group HEALTHSEVERITY -----> this is health severity of the sub group TYPE -----> this represents the type of the group AVAILABILITYSEVERITY -----> this is availability severity of the sub group

Field	Description
	<p>AVAILABILITYMESSAGE -----> this is availability message of the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p> <p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>

```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqlexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqlexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqlexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqlexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqlexpress"

```



```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```



```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```

```

NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group

Field	Description
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this monitor group
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	DetailsPageURL -----> this is details page of the sub group TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group AvailabilityRCAURL -----> this is availability RCA url of the sub group Action -----> this is action status of the sub group NAME \ DISPLAYNAME -----> this is displayname of the sub group TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group HEALTHSEVERITY -----> this is health severity of the sub group TYPE -----> this represents the type of the group AVAILABILITYSEVERITY -----> this is availability severity of the sub group

Field	Description
	<p>AVAILABILITYMESSAGE -----> this is availability message of the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p> <p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>

```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqllexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqllexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqllexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqllexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqllexpress"

```

```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```



```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```



```

NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>

```

ListMGDetails API

This API will fetch the Monitor Group Details of the given monitor group id which includes all the sub-groups and associated monitors configured of the Monitor group. This will also list the monitor groups associated to the user. This will have information about monitor groups today's availability, monitor health outages among subgroups and associated monitors.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListMGDetails?apikey=[API Key]&groupId=10000048`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListMGDetails?apikey=[API Key]&groupName='Test Group'`

Request Parameters:

Field	Description
groupId	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group id for the user
groupName	This parameter is used to get the Monitor Group and its associated monitors based on the monitor group name for the user

Response Details:

Field	Description
NAME \ DISPLAYNAME	This is the displayname of this group
DetailsPageURL	This is the url for the details page of this group
TODAYUNAVAILPERCENT	This the today's unavailability percentage of this group
Action	This represents whether action is enabled or not
TODAYAVAILPERCENT	This the today's availability percentage of this monitor group

Field	Description
TODAYSCHEDDOWNPERCENT	This is the today's scheduled downtime percentage of this monitor group
Type	This represents the type
HEALTHSEVERITY	This represents the severity of the health for this group
AVAILABILITYSEVERITY	This represents the severity of the availability for this group
AVAILABILITYMESSAGE	This represents the availability message for this group
RESOURCEID	This is the resourceid of this group
HealthRCAURL	This is the health RCA url of this group
TODAYUNMANGDPERCENT	This is the today's unmanaged percentage of this monitor group
HEALTHMESSAGE	This represents the health message for this group
HEALTHSTATUS	This is the health status of this group
AVAILABILITYSTATUS	This is the availability status of this group
SubMonitorGroup	DetailsPageURL -----> this is details page of the sub group TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this sub group AvailabilityRCAURL -----> this is availability RCA url of the sub group Action -----> this is action status of the sub group NAME \ DISPLAYNAME -----> this is displayname of the sub group TODAYAVAILPERCENT -----> this is today's availability percentage of the sub group TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the sub group HEALTHSEVERITY -----> this is health severity of the sub group TYPE -----> this represents the type of the group AVAILABILITYSEVERITY -----> this is availability severity of the sub group

Field	Description
	<p>AVAILABILITYMESSAGE -----> this is availability message of the sub group</p> <p>RESOURCEID -----> this is resourceid of the sub group</p> <p>HealthRCAURL -----> this is health RCA url of the sub group</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the sub group</p> <p>HEALTHMESSAGE -----> this is health message of the sub group</p> <p>HEALTHSTATUS -----> this is health status of the sub group</p> <p>AVAILABILITYSTATUS -----> This is the availability status of sub group</p>
Monitors	<p>DetailsPageURL -----> this is details page of the monitor</p> <p>TODAYUNAVAILPERCENT -----> This the today's unavailability percentage of this monitor</p> <p>AvailabilityRCAURL -----> this is availability RCA url of the monitor</p> <p>Action -----> this is action status of the monitor</p> <p>NAME \ DISPLAYNAME -----> this is displayname of the monitor</p> <p>TODAYAVAILPERCENT -----> this is today's availability percentage of the monitor</p> <p>TODAYSCHEDDOWNPERCENT -----> this is today's scheduled downtime percentage of the monitor</p> <p>HEALTHSEVERITY -----> this is health severity of the monitor</p> <p>TYPE -----> this represents the type of the monitor</p> <p>AVAILABILITYSEVERITY -----> this is availability severity of the monitor</p> <p>AVAILABILITYMESSAGE -----> this is availability message of the monitor</p> <p>RESOURCEID -----> this is resourceid of the monitor</p> <p>HealthRCAURL -----> this is health RCA url of the monitor</p> <p>TODAYUNMANGDPERCENT -----> this is today's unmanage percentage of the monitor</p> <p>HEALTHMESSAGE -----> this is health message of the monitorof the monitor</p> <p>HEALTHSTATUS -----> this is health status of the monitor</p> <p>AVAILABILITYSTATUS -----> This is the availability status of the monitor</p>

```

<AppManager-response uri="/AppManager/xml/ListMGDetails">
<result>
<response response-code="4000">
<MonitorGroups>
<MonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000035&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=17" Action="enabled"
NAME="Applications Manager" TODAYAVAILPERCENT="100.0"
TODAYSCHEDDOWNPERCENT="0.0" Type="Monitor Group" HEALTHSEVERITY="1"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource Applications Manager is up.
<br>Root Cause : <br>Resource is Up" RESOURCEID="10000035"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000035&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of Applications Manager is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li><li>Health of appman sub1 is critical. <br>Root Cause :
<br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1. Application Layer
Gateway Service is down<br>2. Application Identity is down<br>3. Application Information is
down<br></li><li></li><li>Health of pavankumar-0549_Tomcat Server_9090 is critical. <br>Root
Cause : <br>1. Average Response Time 2694 > 2000 ms (threshold).<br></li></ol>"
DISPLAYNAME="Applications Manager" HEALTHSTATUS="critical" AVAILABILITYSTATUS="up">
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000042&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=17" Action="enabled"
NAME="127.0.0.1_MS SQL_pavansqlexpress" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="MSSQL-DB-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
127.0.0.1_MS SQL_pavansqlexpress is available." RESOURCEID="10000042"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000042&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of 127.0.0.1_MS
SQL_pavansqlexpress is clear. <br>Root Cause : <br>1. 127.0.0.1_MS SQL_pavansqlexpress is
up<br>2. Buffer Hit Ratio 100 > 90 % (threshold).<br>3. is clear.<br>4. master is ONLINE <br>5.
model is ONLINE <br>6. msdb is ONLINE <br>7. tempdb is ONLINE <br>8. AMDB_10100 is ONLINE
<br>9. AMDB_10030 is ONLINE <br>10. AMDB_test is ONLINE <br>11. syspolicy_purge_history -->
Scheduled Job syspolicy_purge_history. is clear. <br>12. AMDB_app_xp4_admin is ONLINE <br>13.
AMDB_app_xp4_admin1 is ONLINE <br>14. AMDB_pavan_admin is ONLINE <br>15.
AMDB_pavan_MANAGED is ONLINE <br>16. AMDB_imac is ONLINE <br>17. AMDB_ADMIN is
ONLINE <br>18. AMD_10100 is ONLINE <br>19. AMDB_sahad is ONLINE <br>"
HEALTHSTATUS="clear" DISPALYNAME="127.0.0.1_MS SQL_pavansqlexpress"

```

```

AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000045&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=17" Action="enabled"
NAME="AppManager Home Page" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="UrlMonitor"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
AppManager Home Page is available.ResponseCode - 200" RESOURCEID="10000045"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000045&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of AppManager Home Page is clear.
<br>Root Cause : <br>1. AppManager Home Page is up<br>2. Response Time 33 <= 1500 ms
(threshold).<br>" HEALTHSTATUS="clear" DISPALYNAME="AppManager Home Page"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000038&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=17" Action="enabled"
NAME="pavankumar-0549" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="1" TYPE="Windows 7" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource up. <br>The resource pavankumar-0549 is available."
RESOURCEID="10000038" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000038&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549 is critical.
<br>Root Cause : <br>1. Application Layer Gateway Service is down<br>2. Application Identity is
down<br>3. Application Information is down<br>" HEALTHSTATUS="critical"
DISPALYNAME="pavankumar-0549" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000044&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=17" Action="enabled"
NAME="pavankumar-0549-9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Port-Test"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549-9090 is available." RESOURCEID="10000044"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000044&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549-9090 is clear.
<br>Root Cause : <br>1. Response Time 24 <= 1500 ms (threshold).<br>2. pavankumar-0549-9090
is up<br>" HEALTHSTATUS="clear" DISPALYNAME="pavankumar-0549-9090"
AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000043&

```

```

method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Apache Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="5" TYPE="Apache-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Apache Server_9090 is available." RESOURCEID="10000043"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000043&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Apache
Server_9090 is clear. <br>Root Cause : <br>1. pavankumar-0549_Apache Server_9090 is up<br>2.
Response Time 6 <= 1500 ms (threshold).<br>" HEALTHSTATUS="clear"
DISPALYNAME="pavankumar-0549_Apache Server_9090" AVAILABILITYSTATUS="up"/>
<Monitors
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000055&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=17" Action="enabled"
NAME="pavankumar-0549_Tomcat Server_9090" TODAYAVAILPERCENT="100"
TODAYSCHEDDOWNPERCENT="0" HEALTHSEVERITY="1" TYPE="Tomcat-server"
AVAILABILITYSEVERITY="5" AVAILABILITYMESSAGE="Resource up. <br>The resource
pavankumar-0549_Tomcat Server_9090 is available." RESOURCEID="10000055"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10000055&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="Health of pavankumar-0549_Tomcat
Server_9090 is critical. <br>Root Cause : <br>1. Average Response Time 2694 > 2000 ms
(threshold).<br>" HEALTHSTATUS="critical" DISPALYNAME="pavankumar-0549_Tomcat
Server_9090" AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10000267&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=17" Action="enabled"
NAME="appman sub1" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="1" TYPE="Sub Group" AVAILABILITYSEVERITY="5"
AVAILABILITYMESSAGE="Resource appman sub1 is up. <br>Root Cause : <br>Resource is Up"
RESOURCEID="10000267" HealthRCAURL="/jsp/RCA.jsp?resourceid=10000267&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="Health of appman sub1 is critical.
<br>Root Cause : <br><ol><li>Health of pavankumar-0549 is critical. <br>Root Cause : <br>1.
Application Layer Gateway Service is down<br>2. Application Identity is down<br>3. Application
Information is down<br></li></ol>" HEALTHSTATUS="critical" DISPALYNAME="appman sub1"
AVAILABILITYSTATUS="up"/>
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001149&
method=showApplication" TODAYUNAVAILPERCENT="0.0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=17" Action="enabled"

```



```
NAME="Opman" TODAYAVAILPERCENT="100.0" TODAYSCHEDDOWNPERCENT="0.0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001149"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001149&attributeid=18"
TODAYUNMANGDPERCENT="0.0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="Opman" AVAILABILITYSTATUS="UnKnown">
<SubMonitorGroup
DetailsPageURL="/showresource.do?method=showResourceForResourceID&resourceid=10001151&
method=showApplication" TODAYUNAVAILPERCENT="0"
AvailabilityRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=17" Action="enabled"
NAME="123" TODAYAVAILPERCENT="100" TODAYSCHEDDOWNPERCENT="0"
HEALTHSEVERITY="-" TYPE="Sub Group" AVAILABILITYSEVERITY="-"
AVAILABILITYMESSAGE="-" RESOURCEID="10001151"
HealthRCAURL="/jsp/RCA.jsp?resourceid=10001151&attributeid=18"
TODAYUNMANGDPERCENT="0" HEALTHMESSAGE="-" HEALTHSTATUS="UnKnown"
DISPALYNAME="123" AVAILABILITYSTATUS="UnKnown"/>
</MonitorGroup>
</MonitorGroups>
</response>
</result>
</AppManager-response>
```


ListActions API

This API lists all the actions configured for the monitors associated to the users. The details of each action is grouped according to the action type.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/ListActions?apikey=[API Key]&type=all`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/ListActions?apikey=[API Key]&type='all'`

In future versions the following features will be included:

- i) Listing Actions will be supported in Admin server.*
- ii) Listing Actions based on the type.*

Request Parameters:

Field	Description
type	This value specifies the type of action to be listed, to get all types of actions, we need to pass 'all' as the value for the field type.(In absence of this parameter also it will return all the types)

Response Details:

Field	Description
DisplayName	This is the displayname of the action.
Action	ID - Represents the Action ID ExecuteActionPath - Represents the uri for executing the action NAME - Represents the Name of the Action ActionProps - Represents the Action Properties like From Address, To Address, Message etc., this changes for each and every action type

```
<AppManager-response uri="/AppManager/xml/ListActions">
<result>
<response response-code="4000">
<Actions DisplayName="SMS Action(s)">
<Action ID="10000003"
ExecuteActionPath="/common/executeSMS.do?method=testAction&remote=true&actionID=10000003"
NAME="SMS">
<ActionProps MESSAGE="This information has been generated by the Applications Manager"
FROMADDRESS="karthi@zohomail.com" TOADDRESS="karthi@zohomail.com" />
</Action>
</Actions>
</response>
</result>
</AppManager-response>
```

Search API

This API will fetch the List of Monitors / Monitor Groups that matches the query string. Also the search will be with in the list of monitors assigned to the user.

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/Search?apikey=[API Key]&query='pavan'`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/Search?apikey=[API Key]&query='pavan'`

Request Parameters:

Field	Description
query	This value specifies the string that has to be searched in the monitors list associated to an user.

Response Details:

Field	Description
Type	This represents the type of the element got in search results
HealthStatus	This is health status of the search element
AvailabilityMessage	This is the availability message of the search element
DisplayName	This is the displayname of the search element
ManagedServer	This is the managed server name in which the monitor or group is added.It will have 'NA' as value for professional edition
AvailabilityStatus	This is availability status of the search element
SubGroup	This is category to which the elements belongs to.
ResourceId	This is the resource id of the search element.

Field	Description
HealthMessage	This is the health message of the search element
HealthSeverity	This is the health severity of the search element
ImagePath	This is monitor type/ monitor group image path
AvailabilitySeverity	This is the availability severity of the search element
DetailsPageURL	This is details page of the search element.

```

<AppManager-response uri="/AppManager/xml/Search">
<result>
<response response-code="4000">
<Monitor Type="EC2Instance" HealthStatus="clear" AvailabilityMessage="Resource down. <br>The
resource APM_10 is not available." DisplayName="APM_10" ManagedServer="Admin Server"
AvailabilityStatus="down" SubGroup="EC2Instance" ResourceId="10000406"
HealthMessage="Cleared by User" HealthSeverity="5"
ImagePath="/images/icon_monitor_ec2_ins.gif" AvailabilitySeverity="1"
DetailsPageURL="/showresource.do?resourceid=10000406&method=showResourceForResourceID&
PRINTER_FRIENDLY=true"/>
<Monitor Type="EC2Instance" HealthStatus="clear" AvailabilityMessage="Resource up. <br>The
resource Apm-Insight Beta version is available." DisplayName="Apm-Insight Beta version"
ManagedServer="Admin Server" AvailabilityStatus="up" SubGroup="EC2Instance"
ResourceId="10000407" HealthMessage="Health of Apm-Insight Beta version is clear. <br>Root
Cause : <br>1. Apm-Insight Beta version is up<br>2. vol-68491f01 --> <br>" HealthSeverity="5"
ImagePath="/images/icon_monitor_ec2_ins.gif" AvailabilitySeverity="5"
DetailsPageURL="/showresource.do?resourceid=10000407&method=showResourceForResourceID&
PRINTER_FRIENDLY=true"/>
<Monitor Type="APM-Insight-Instance" HealthStatus="critical" AvailabilityMessage="Resource down.
<br>The resource hemachand-0591:8080 is not available." DisplayName="hemachand-0591:8080"
ManagedServer="Admin Server" AvailabilityStatus="down" SubGroup="APM-Insight-Instance"
ResourceId="10007308" HealthMessage="Resource hemachand-0591:8080 is down. <br>Health is
critical as the resource is not available" HealthSeverity="1"
ImagePath="/apminsight/images/apminsight-icon.gif" AvailabilitySeverity="1"
DetailsPageURL="/showresource.do?resourceid=10007308&method=showResourceForResourceID&
PRINTER_FRIENDLY=true"/>
<Monitor Type="Windows XP" HealthStatus="clear" AvailabilityMessage="Resource up. <br>The
resource APM-Windows is available." DisplayName="APM-Windows" ManagedServer="Admin
Server" AvailabilityStatus="up" SubGroup="Windows" ResourceId="10001267"

```

```
HealthMessage="Health of APM-Windows is clear. <br>Root Cause : <br>1. Data Collection  
Successful<br>2. APM-Windows is up<br>" HealthSeverity="5"  
ImagePath="/images/icon_monitors_windows.gif" AvailabilitySeverity="5"  
DetailsPageURL="/showresource.do?resourceid=10001267&method=showResourceForResourceID&  
PRINTER_FRIENDLY=true"/>  
</response>  
</result>  
</AppManager-response>
```

ShowPolledData API

This API will fetch the List of Dashboards created in the Server which includes all the widgets configured in the Dashboards as there is no concept of assigning the dashboards/widgets to operators. But the data which is gonna be populated will be based on the monitors assigned for the user.

API for XML Response:

http://[APM Host]:[APM Port]/AppManager/xml/ShowPolledData?apikey=[API Key]

API for JSON Response:

http://[APM Host]:[APM Port]/AppManager/json/ShowPolledData?apikey=[API Key]

Request Parameters:

Field	Description
resourceid	This value is the resourceid of the monitor from which the data has to be fetched.
attributeID	This is the value of the attribute id for which the polled or archived data has to be shown.
period	This value specifies the the type of data that needs to be returned. its values are : 20 for show polled data, -7 for 7 days archived data and -30 for 30 days archived data.

Example urls:

Polled Data:

API for XML Response:

http://[APM Host]:[APM Port]/AppManager/xml/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=20&attributeID=310

API for JSON Response:

http://[APM Host]:[APM Port]/AppManager/json/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=20&attributeID=3102

Last 7 days Data:

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=-7&attributeID=3102`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=-7&attributeID=3102`

Last 30 days Data:

API for XML Response:

`http://[APM Host]:[APM Port]/AppManager/xml/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=-30&attributeID=3102`

API for JSON Response:

`http://[APM Host]:[APM Port]/AppManager/json/showPolledData?apikey=8c8ec3f2cd30722d3a6f980df12c1e5f&resourceid=10000042&period=-30&attributeID=3102`

Response Details:

Field	Description
StartTime	This is the start time in milli seconds format from which 7/30/ show polled data report is generated
EndTime	This is the end time in milli seconds format from which 7/30/ show polled data report is generated
StartDateTime	This is the start time in date time format from which 7/30/ show polled data report is generated
EndDateTime	This is the end time in date time format from which 7/30/ show polled data report is generated
ResourceName	This is the monitor name from which the data is returned
ResourceType	This is the type of the resource for which the data is returned
AttributeName	This is the name of the attribute
Unit	This is the units of the attribute
AttributeID	This is the ID of the user
ReportType	This is the type of data this API call is returning (Polled data / 7 days data / 30 days data).

Field	Description
BusinessPeriod	This represents the business period name
ResourceId	This is the monitor resourceid
AttributeImage	This is the attribute graph for the data returned along with this response.
Status	This is the status of the REST API call to get the show polled data
Period	This value specifies the the type of data that needs to be returned. its values are : 20 for show polled data, -7 for 7 days archived data and -30 for 30 days archived data.
RawData	CollectionTime -- represents the time stamp in ms at which the data is collected DateTime -- represents the time stamp in date time format at which the data is collected Value -- this represents the value of the attribute
ArchiveData	ArchivedTime -- represents the archived time in ms DateTime -- represents the archived time in date time format AvgValue -- this is the avg time of the value in that archived period MinValue -- this is the minimum value in that archived period MaxValue -- this is the maximum value in that archived period

```

<AppManager-response uri="/AppManager/xml/ShowPolledData">
<result>
<response response-code="4000">
<Monitorinfo StartTime="1328775260450" EndDateTime="Mar 29, 2012 3:00 PM"
ResourceName="APM-Windows" Unit="ms" EndTime="1333013434474" BusinessPeriod="NA"
MonitorType="Response Time" ReportType="Polled data" ResourceId="10001267"
AttributeID="4602" AttributeImage="/webclient/temp/images/RSVmYs.jpg" ServerType="GlassFish"
Status="SUCCESS" StartDateTime="Feb 9, 2012 1:44 PM" Period="20">
<RawData CollectionTime="1333013434474" Value="1" DateTime="Mar 29, 2012 3:00 PM"/>
<RawData CollectionTime="1333013134022" Value="1" DateTime="Mar 29, 2012 2:55 PM"/>
<RawData CollectionTime="1333012833497" Value="1" DateTime="Mar 29, 2012 2:50 PM"/>
<RawData CollectionTime="1333012532708" Value="1" DateTime="Mar 29, 2012 2:45 PM"/>
<RawData CollectionTime="1333012227193" Value="1" DateTime="Mar 29, 2012 2:40 PM"/>
<RawData CollectionTime="1328775260450" Value="1" DateTime="Feb 9, 2012 1:44 PM"/>
</Monitorinfo>
</response>
</result>
</AppManager-response>

```


Ping API

This API will be used to ping the given server or the server corresponding to the given monitor's resourceid. The ping command will be executed and the result will be passed as response of the request.

API for XML Response:

*http://[APM Host]:[APM Port]/AppManager/xml/**Ping**?apikey=[API Key]&resourceid='10000157'*

API for JSON Response:

*http://[APM Host]:[APM Port]/AppManager/json/**Ping**?apikey=[API Key]&host='hemachand-0591'*

Request Parameters:

Field	Description
resourceid	This value specifies the resourceid of the monitor, So that we can ping host corresponding to monitor.
host	This is the host of any server which can be passed as parameter to ping from the Applications Manager server.

Response Details:

Field	Description
APIKey	This is the username.
Description	This is the description of the user account given at the time of creation of user account
EmailID	This is the e-mail id of the user
GroupName	This is the typ of account the user has. ex: operator, admin, manager etc.,
UserImage	This is User image path
UserID	This is the ID of the user
UserName	This is the username of the user.

```
<AppManager-response uri="/AppManager/xml/Ping">
<result>
<response response-code="4000">
<PingResult Output="Pinging 127.0.0.1 with 32 bytes of data:<br>Reply from 127.0.0.1: bytes=32
time<1ms TTL=128<br><br>Ping statistics for 127.0.0.1:<br>Packets: Sent = 1, Received = 1, Lost =
0 (0% loss),<br>Approximate round trip times in milli-seconds:<br>Minimum = 0ms, Maximum = 0ms,
Average = 0ms<br>" Host="127.0.0.1" IPAddress="127.0.0.1"/>
</response>
</result>
</AppManager-response>
```

MaintenanceTask

MaintenanceTask API

The APIs given below allow you to work with downtime schedules in Applications Manager:

- CreateMaintenanceTask
- EditMaintenanceTask
- DeleteMaintenanceTask
- GetMaintenanceTaskDetails

Request Parameters

The common parameters involved in these API requests are described below:

Field	Description
apikey	The key generated from the Generate API Key option in the 'Admin' tab.
taskName	The name of the maintenance task. This should be a unique value.
taskType	The type of task to be created. The options are monitor and group
taskStatus	Current status of the schedule. You have to choose from either 'enable' or 'disable'
taskid	The unique identifier for the task
resourceid	The resource id of the monitor for which the schedule has to be created

Sample Request:

This example helps you to create a downtime schedule in Applications Manager:

```
http://app-windows:9090/AppManager/xml/CreateMaintenanceTask?apikey=bdd4d0643c6f591e123b7ba6fb69d9dd&taskMethod=daily&taskStartTime=20:00&taskEndTime=21:00&taskStatus=disable&taskEffectFrom=2010-05-24%2016:48&taskName=dr1&taskType=monitor&resourceid=10000055
```

If the API is not executed correctly, the request will fail and errors will be thrown. Refer this page for a list of common error conditions.

CreateMaintenanceTask API

This API allows the user to create downtime schedules in Applications Manager. The schedules can be created with any of the following recurrence types:

- Daily
- Weekly
- Once

Downtime Schedule with Recurring type Daily

Sample Request:

```
http://[Host]:[Port]/AppManager/xml/CreateMaintenanceTask?apikey=[APIKEY]&taskMethod=daily&taskStartTime=[STARTTIME]&taskEndTime=[ENDTIME]&taskStatus=disable&taskEffectFrom=[DATE]&taskName=[NAME]&taskType=monitor&resourceid=[RESOURCEID]
```

Request Parameters

The parameters involved in this API request are described below. Also, refer the list of common Request Parameters involved in executing the CreateMaintenanceTask API requests.

Field	Description
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'daily' indicates the schedule runs every day.
taskStartTime	The time when the maintenance task starts running
taskEndTime	The time when the maintenance task stops running
taskEffectFrom	The date and time from which the maintenance task becomes active

Example:

```
http://app-windows:9090/AppManager/xml/CreateMaintenanceTask?apikey=bdd4d0643c6f591e123b7ba6fb69d9dd&taskMethod=daily&taskStartTime=20:00&taskEndTime=21:00&taskStatus=disable&taskEffectFrom=2010-05-24%2016:48&taskName=dr1&taskType=monitor&resourceid=10000055
```

Output for the above example:

```
<AppManager-response uri="/AppManager/xml/CreateMaintenanceTask">
  <result>
    <response response-code="4000">
      <message>Maintenance Task successfully created.</message>
    </response>
  </result>
</AppManager-response>
```

Downtime Schedule with Recurring type Weekly

Sample Request:

```
http://[Host]:[Port]/AppManager/xml/CreateMaintenanceTask?apikey=[APIKEY]&taskType=[TASKTYPE]&resourceid=[RESOURCEID]
&totalNumber=[TOTALNUMBER]&taskMethod=[TASKMETHOD]&taskDescription=[TASKDESCRIPTION]&taskStatus=[TASKSTATUS]
&taskEffectFrom=[DATETIME]&startDay1=[STARTDAY1]&startTime1=[STARTTIME1]&endDay1=[ENDDAY1]&endTime1=[ENDTIME1]
&taskName=[TASKNAME]
```

Request Parameters

The parameters involved in the API request are described below:

Field	Description
totalNumber	The number of schedules to be created. You can create a maximum of 7 weekly schedules
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'weekly' indicates the schedule runs every week.
taskDescription	The description of what the maintenance schedule does, optional value.
taskEffectFrom	The date and time from which the maintenance task becomes active
startDay[n]	The day on which the maintenance task starts running. The allowed values for n are 1,2,3,4,5,6 and 7
startTime[n]	The time when the maintenance task starts running. The allowed values for n are 1,2,3,4,5,6 and 7
endDay[n]	The day on which the maintenance task stops running. The allowed values for n are 1,2,3,4,5,6 and 7
endTime[n]	The time at which the maintenance task stops running. The allowed values for n are 1,2,3,4,5,6 and 7

Example:

```
http://app-
windows:9090/AppManager/xml/CreateMaintenanceTask?apikey=983a7d7ed56c5753f4977df5883e2b2d&taskT
ype=monitor
&resourceid=10000028&totalNumber=1&taskMethod=weekly&taskDescription=&taskStatus=disable&taskEffectF
rom=2010-06-01%2011:25
&startDay1=tuesday&startTime1=10:00&endDay1=friday&endTime1=12:00&taskName=week
```

You can create up to 7 weekly schedules at one go.

Downtime Schedule with Recurring type Once**Sample Request:**

```
http://[Host]:[Port]/AppManager/xml/CreateMaintenanceTask?apikey=[APIKEY]&taskMethod=[TASKMETHOD]&c
ustomTaskStartTime=[CUSTOMTASKSTARTTIME]
&customTaskEndTime=[CUSTOMTASKENDTIME]&taskStatus=[TASKSTATUS]&taskName=[TASKNAME]&task
Type=[TASKTYPE]
&taskDescription=[TASKDESCRIPTION]&resourceid=[RESOURCEID]
```

Request Parameters

The parameters involved in this API request are described below. Also, refer the list of common Request Parameters involved in executing the API requests.

Field	Description
API Key	The key generated from "Generate API Key" option in the Admin tab.
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'weekly' indicates the schedule runs every week.
customTaskStartTime	The date and time when the schedule starts running
customTaskEndTime	The date and time when the schedule stops running
taskDescription	The description of what the maintenance schedule does. This parameter is optional.

Example:

```
http://app-
windows:9090/AppManager/xml/CreateMaintenanceTask?apikey=095cb3835ff015b01a3b3a6c4ab2c38a&taskM
ethod=once
&customTaskStartTime=2010-06-03%2012:46&customTaskEndTime=2010-06-
05%2012:46&taskStatus=disable&taskName=once
&taskType=monitor&taskDescription=&resourceid=10000322
```

EditMaintenanceTask API

This API allows the user to edit downtime schedules in Applications Manager. Users can edit schedules with the following recurring types:

- Daily
- Weekly
- Once

Editing Downtime Schedule with Recurring type Daily

Sample Request:

```
http://[Host]:[Port]/AppManager/xml/EditMaintenanceTask?apikey=[APIKEY]&taskMethod=[TASKMETHOD]&taskStartTime=[TASKSTARTTIME]&taskEndTime=[TASKENDTIME]&taskStatus=[TASKSTATUS]&taskEffectFrom=[TASKEFFECTFROM]&taskName=[TASKNAME]&taskType=[TASKTYPE]&resourceid=[RESOURCEID]&taskid=[TASKID]
```

Request Parameters

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters involved in executing the EditMaintenanceTask API requests.

Field	Description
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'daily' indicates the schedule runs every day.
taskStartTime	The time when the maintenance task starts running
taskEndTime	The time when the maintenance task stops running
taskEffectFrom	The date and time from which the maintenance task becomes active

Example:

```
http://app-windows:9090/AppManager/xml/EditMaintenanceTask?apikey=095cb3835ff015b01a3b3a6c4ab2c38a&taskMethod=daily&taskStartTime=20:00&taskEndTime=21:00&taskStatus=enable&taskEffectFrom=2010-06-05%2016:48&taskName=june4a&taskType=monitor&resourceid=10000059&taskid=10000003
```

Example output:

```
<AppManager-response uri="/AppManager/xml/EditMaintenanceTask">
  <result>
    <response response-code="4000">
      <message>Maintenance Task successfully edited.</message>
```

```

</response>
</result>
</AppManager-response>

```

Editing Downtime Schedule with Recurring type Weekly

Sample Request:

```

http://[Host]:[Port]/AppManager/xml/EditMaintenanceTask?apikey=[APIKEY]&taskType=[TASKTYPE]&resourceid
=[RESOURCEID]&totalNumber=[TOTALNUMBER]
&taskMethod=[TASKMETHOD]&taskDescription=[TASKDESCRIPTION]&taskStatus=[TASKSTATUS]&taskEffect
From=[DATETIME]&startDay1=[STARTDAY1]
&startTime1=[STARTTIME1]&endDay1=[ENDDAY1]&endTime1=[ENDTIME1]&taskName=[TASKNAME]&taskid
=[TASKID]

```

Request Parameters

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters involved in executing the EditMaintenanceTask API requests.

Field	Description
totalNumber	The number of schedules to be created. You can create a maximum of 7 weekly schedules
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'weekly' indicates the schedule runs every week.
taskDescription	The description of what the maintenance schedule does, optional value.
taskEffectFrom	The date and time from which the maintenance task becomes active
startDay[n]	The day on which the maintenance task starts running. The allowed values for n are 1,2,3,4,5,6 and 7
startTime[n]	The time when the maintenance task starts running. The allowed values for n are 1,2,3,4,5,6 and 7
endDay[n]	The day on which the maintenance task stops running. The allowed values for n are 1,2,3,4,5,6 and 7
endTime[n]	The time at which the maintenance task stops running. The allowed values for n are 1,2,3,4,5,6 and 7

Example:

```
http://app-
windows:9090/AppManager/xml/EditMaintenanceTask?apikey=095cb3835ff015b01a3b3a6c4ab2c38a&taskType
=monitor
&resourceid=10000028&totalNumber=1&taskMethod=weekly&taskDescription=&taskStatus=enable&taskEffectFr
om=2010-06-01%2011:25
&startDay1=tuesday&startTime1=10:00&endDay1=friday&endTime1=12:00&taskName=week1&taskid=1000000
4
```

Downtime Schedule with Recurring type Once**Sample Request:**

```
http://[Host]:[Port]/AppManager/xml/EditMaintenanceTask?apikey=[APIKEY]&taskMethod=[TASKMETHOD]&cust
omTaskStartTime=[CUSTOMTASKSTARTTIME]
&customTaskEndTime=[CUSTOMTASKENDTIME]&taskStatus=[TASKSTATUS]&taskName=[TASKNAME]&task
Type=[TASKTYPE]
&taskDescription=[TASKDESCRIPTION]&resourceid=[RESOURCEID]&taskid=[TASKID]
```

Request Parameters

The parameters involved in the API request are described below:

Field	Description
taskMethod	Denotes the recurring frequency of the maintenance schedule, 'weekly' indicates the schedule runs every week.
customTaskStartTime	The date and time when the schedule starts running
customTaskEndTime	The date and time when the schedule stops running
taskDescription	The description of what the maintenance schedule does. This parameter is optional.

Example:

```
http://app-
windows:9090/AppManager/xml/EditMaintenanceTask?apikey=095cb3835ff015b01a3b3a6c4ab2c38a&taskMeth
od=once
&customTaskStartTime=2010-06-03%2012:46&customTaskEndTime=2010-06-
05%2012:46&taskStatus=enable&taskName=once1
&taskType=monitor&taskDescription=&resourceid=10000322&taskid=10000005
```

DeleteMaintenanceTask API

This API allows the user to delete a downtime schedule in Applications Manager.

Sample Request

http://[Host]:[Port]/AppManager/xml/DeleteMaintenanceTask?apikey=[APIKEY]&taskid=[TASKID]

Request Parameters

The parameters involved in the API request are described below:

Field	Description
API Key	The key generated from "Generate API Key" option in the Admin tab.
taskid	The TASKID in the AM_MAINTENANCECONFIG table

Example:

http://app-windows:9090/AppManager/xml/DeleteMaintenanceTask?apikey=5bc6a8e9a30d5bf894586d4db90282f5&taskid=10000001

Output for the above example:

```
<AppManager-response uri="/AppManager/xml/DeleteMaintenanceTask">
  <result>
    <response response-code="4000">
      <message>Maintenance Task successfully deleted.</message>
    </response>
  </result>
</AppManager-response>
```

GetMaintenanceTaskDetails/ListMaintenanceTaskDetails API

This API allows the user to view the details of downtime schedules configured in Applications Manager.

Sample Request

http://[Host]:[Port]/AppManager/xml/ListMaintenanceTaskDetails?apikey=[APIKEY]

Request Parameters

The parameters involved in the API request are described below:

Field	Description
apikey	The key generated from "Generate API Key" option in the Admin tab.

Example:

http://app-windows:9090/AppManager/xml/ListMaintenanceTaskDetails?apikey=93c6eb60184e41f10fba2f365060b8e3

Output for the above example:

```
<AppManager-response uri="/AppManager/xml/ListMaintenanceTaskDetails">
  <result>
    <response response-code="4000">
      <Schedules>
        <Schedule TASKNAME="Test_Weekly" TASKID="10000001" STATUS="RUNNING" OCCURENCE="Weekly">
          <ScheduledTime STARTTIME="Monday 20:00" ENDTIME="Wednesday 20:00" />
          <ScheduledTime STARTTIME="Tuesday 14:00" ENDTIME="Wednesday 15:00" />
        </Schedule>
      </Schedules>
    </response>
  </result>
</AppManager-response>
```

GetMonitorData API

This API allows the user to fetch the data for the latest poll from monitors. At the moment, we support fetching of first-level attributes of a monitor, i.e. the current data for the important attributes of a monitor such as response time, collection time, etc.

Sample Request:

`http://[Host]:[Port]/AppManager/xml/GetMonitorData?apikey=[APIKEY]&resourceid=[RESOURCEID]`

Request Parameters

The parameters involved in the API request are described below:

Field	Description
API Key	The key generated from "Generate API Key" option in the Admin tab.
resourceid	The resource id of the monitor for which data needs to be fetched

Example:

`http://app-windows:9090/AppManager/xml/GetMonitorData?apikey=095cb3835ff015b01a3b3a6c4ab2c38a&resourceid=10000293`

The above example fetches the current data of a Sybase monitor.

Output for the above example:

```
<AppManager-response uri="/AppManager/xml/GetMonitorData">
  <result>
    <response response-code="400">
      <Monitorinfo DISPLAYNAME="app-xp3.zohocorpin.com_SYBASE-DB-server_5000" RESOURCEID="10000322"
      TYPE="SYBASE-DB-server"/>
      <Attribute DISPLAYNAME="Connection Time" Value="8" Units=" ms" AttributeID="8502"/>
      <Attribute DISPLAYNAME="Active Remote Connections" Value="0" Units=" " AttributeID="8508"/>
      <Attribute DISPLAYNAME="Active User Connections" Value="3" Units=" " AttributeID="8509"/>
      <Attribute DISPLAYNAME="Total Memory" Value="79872" Units=" KB" AttributeID="8503"/>
      <Attribute DISPLAYNAME="Memory Used" Value="57042" Units=" KB" AttributeID="8504"/>
      <Attribute DISPLAYNAME="Free Memory" Value="22830" Units=" KB" AttributeID="8505"/>
      <Attribute DISPLAYNAME="Used Memory Percentage" Value="71.42" Units=" %" AttributeID="8506"/>
    </response>
  </result>
</AppManager-response>
```

AddMonitor

AddMonitor API

This API allows the user to configure monitors in Applications Manager.

Request Parameters

The common parameters involved in the API request are described below:

Field	Description
apikey*	The key generated from the Generate API Key option in the 'Admin' tab.
displayname*	The display name of the monitor.
subnet	The subnet where the server is running. The default value is 225.225.225.0.
pollInterval	The interval at which the server needs to be polled. The default value is 5 minutes.
addToGroup	Denotes whether the monitor should be added as part of a monitor group or not. The value can be either 'True' or 'False'.
groupID	The id of the monitor group. This has to be provided if 'addToGroup' value is 'True'.

* - mandatory

Sample Request

This example helps you add a Windows server to Applications Manager:

```
http://app-
windows:9090/AppManager/xml/AddMonitor?apikey=0b0fd47feeff9050d6a45dd7b5bb5791&type=ser
vers&displayname=APM-Windows&host=app-
xp4&snmpTelnetport=161&os=WindowsXP&mode=SNMP&username=administrator&password=vemb
u
```

Example output:

```
<AppManager-response uri="/AppManager/xml/AddMonitor">
  <result>
    <response response-code="4000">
      <message>Monitor added successfully.</message>
    </response>
  </result>
</AppManager-response>
```

Sample Error

If the API is not executed correctly, the request will fail and errors will be thrown as shown below.

```
<Apm-response uri="/AppManager/xml/AddMonitor">
  <result>
    <response response-code="4225">
      <message>The Transaction mentioned in the request URL should be yes or no.</message>
    </response>
  </result>
</Apm-response>
```

Refer this page for a list of common error conditions.

AddMonitor API - Application Servers

This section explains how to use the AddMonitor API to add monitors of the 'Application Servers' category. The following application servers are supported:

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

Microsoft .NET

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be '.Net'.
host	The name of the host where the .Net server is running.
username	The username of the .Net server.
password	The password of the .Net server.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=4df5040d6db873dcdaf4359b259fd
494
&type=.net&displayname=AppmanagerDotNet&host=app-
xp3&username=administrator&password=vembu
```

GlassFish

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
host=[HOST]
&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&displayname=[DISPLAYNA
ME]&JNDIPath=[JNDIPATH]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'glassfish'.
host	The name of the host where the GlassFish server is running.
port	The port number where GlassFish server is running.
username	The username of the GlassFish server.
password	The password of the GlassFish server.
JNDIPath	The JNDI path name. For example, the JNDIPATH for default installations of GlassFish is /jmxrmi.

Sample Request:

```
http://prod-
server1:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273
313
&type=glassfish&host=app-xp2&port=8686&username=admin&password=adminadmin
&displayname=glfish&JNDIPath=/jmxrmi
```

JBoss Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]
&version=[VERSION]&authEnabled=[AUTHENABLED]&username=[USERNAME]&password=[
PASSWORD]
```


Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'JBoss server'.
host	The name of the host where the JBoss server is running.
port	The port number where JBoss server is running.
version	The version of the JBoss server. Supported versions include 3.2.x, 4.x, 4.0.1, 4.0.2 and 5.0.0
authEnabled	Denotes whether authentication is enabled in the JBoss server. Value should be either 'on' or 'off'
username	The username of the JBoss server. This should be specified only if authEnabled value is 'on'.
password	The password of the JBoss server. This should be specified only if authEnabled value is 'on'

Sample Request:

```
http://prod-server2:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=JBoss server&displayname=AppmanagerJBoss&host=app-
xp2&port=8080&version=4.0.2&authEnabled=on&username=guest&password=guest
```

Oracle Application Server**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&version=[VERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	Denotes the category type of the monitor you want to add. If you want to add a WebLogic monitor, specify the value as 'WEBLOGICSERVER'.
host	The name of the host where the Oracle application server is running.
port	The port number where Oracle application server is running.
version	The version of the Oracle application server. Supported version is 10.1.3

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=oracle application server&displayname=appmanageroracle&host=app-
xp5&port=7200&version=10.1.3
```

SilverStream Server**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST] &port=[PORT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'SilverStream'
host	The name of the host where the SilverStream server is running.
port	The port number where the SilverStream server is running.

Sample Request:

```
http://prod-server6:8090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=SilverStream&displayname=sl&host=myesuraj&port=8080
```

Tomcat Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&version=[VERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. The value should be 'tomcat server'.
host	The name of the host where the Tomcat server is running.
port	The port number where Tomcat is running.
username	The username of the Tomcat server.
password	The password of the Tomcat server.
version	The version of the Tomcat server. Supported version is 5.

Sample Request:

```
http://app-
xp5:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=tomcat
server&displayname=appmanagertomcat&host=shakthiprian&port=8080&username=admin&password=admin&version=5
```

WebLogic Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&version=[VERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	Denotes the category type of the monitor you want to add. The value should be as 'WEBLOGICSERVER'.

Field	Description
host	The name of the host where the WebLogic is running.
port	The port number where WebLogic is running.
username	The username of the WebLogic server.
password	The password of the WebLogic server.
version	The version of the WebLogic server. Supported versions include 6.1, 7.0, 8.1, 9.x and 10.x

Sample Request

```
http://app-
windows:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273
313
&type=WEBLOGIC_SERVER&displayname=Appmanagerweblogic&host=app-
linux1&port=7001&username=weblogic
&password=weblogic&version=8.1
```

WebSphere Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&port=[PORT]&version=[VERSION]&mode=[MODE]&soapport=[SOAPPORT]
```

Request Parameters:

Field	Description
type	Denotes the category type of the monitor you want to add. The value should be 'websphere server'.
host	The name of the host where the WebSphere is running.
port	The port number where WebSphere is running.
username	The username of the WebSphere server.
password	The password of the WebSphere server.
version	The version of the WebSphere server. Supported versions include 6.x
mode	The deployment mode of the server. Value is 'BASE'
soapport	The SOAP connector port.

Sample Request:

```
http://prod-  
server4:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273  
313  
&type=websphere server&displayname=Appmanagerwebsphere&host=app-  
xp4&port=9080&version=6.x&mode=base&soapport=888
```

AddMonitor API - ERP

This section explains how to use the AddMonitor API to add monitors of the 'ERP' category type. The following monitors are supported:

- Oracle EBS
- SAP Server

Oracle EBS

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&SSL=[SSL]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the ERP server you want to add. Value should be OracleEBS.
host	The name of the host in which Oracle EBS is running.
port	The port number where the Oracle EBS is running.
SSL	Indicates if SSL option is enabled. The value should be either yes or no.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=4df5040d6db873dcdaf4359b259fd494&type=OracleEBS&displayname=oebs&host=app-xp2&port=80&SSL=no
```

SAP Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&username=[USERNAME]&password=[PASSWORD]&systemnumber=[SYSTEMNUMBER]&logonClient=[LOGONCLIENT]&language=[LANGUAGE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the ERP server you want to add. Value should be sap server.
host	The name of the host in which SAP server is running.
username	The user name used for accessing the SAP server.
password	The password of the SAP server.
systemnumber	The SAP system number.
logonClient	The SAP logon client.
language	The SAP logon language. Default value is en.

Sample Request:

```
http://prod-server1:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=sap_server&displayname=appmanagersap&host=app-xpl&username=BCUSER&password=minisap&systemnumber=00&logonClient=000&language=en
```

AddMonitor API - Java/Transaction

This section explains how to use the AddMonitor API to add monitors of the category type 'Java/Transaction'. The following monitors are supported:

- Java Runtime
- J2EE Web Transactions

Java Runtime

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&jndiurl=[JNDIURL]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Java Runtime.
host	The name of the host where the monitor is running.
port	The port number where the Java Runtime monitor is running.
jndiurl	The JNDI name. The default value is jmxrmi.

Sample Request:

```
http://op-
server5:9090/AppManager/xml/AddMonitor?apikey=4df5040d6db873dcda4359b259fd
494
&type=Java
Runtime&displayname=apmjava&host=myesuraj&port=1099&jndiurl=/jmxrmi
```

J2EE Web Transactions

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&jndiurl=[JNDIURL]
```


Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be J2EE Web Transactions
host	The name of the host where the monitor is running.
port	The port number where the J2EE Web Transaction monitor is running.

Sample Request:

```
http://prod-server4:9090/AppManager/xml/AddMonitor?apikey=90c166a4646e29315a57ecald6b88858&type=J2EE Web Transactions&displayname=apmjavaee&host=app-xp2&port=55555
```

AddMonitor API - Servers

This section explains how to use the AddMonitor API to add monitors of the category type 'Servers'.

The following servers are supported:

- AIX
- AS400
- FreeBSD/OpenBSD
- HP-UX/Tru64
- Linux
- Mac OS
- Novell
- Sun Solaris
- Windows

AIX

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&os=[OS]&username=[USERNAME]&mode=[MODE]&snmp telnet port=[SNMPTELNETPORT]&pa
ssword=[PASSWORD]&prompt=[PROMPT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the AIX server is running.
os	The operating system of the server. Value is 'AIX'.
username	The username of the AIX server.
mode	The mode of monitoring the AIX server. Value is 'TELNET'.
snmp telnet port	The port number where Telnet service is running. Default value is 23.
password	The password of the AIX server.
prompt	The command prompt value. Value is '\$'

Sample Request:

```
http://prod-server1:9098/AppManager/xml/AddMonitor?apikey=624436f73f9fda2109cc916c8c8be5c1&type=servers
&displayname=apmaix&host=adventaix&os=AIX&username=root&mode=TELNET&snmpTelnetport=23&password=sankho&prompt=#
```

AS400**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&subnet=[SUBNET]&pollInterval=[POLLINTERVAL]&os=[OS]&username=[USERNAME]&pa
ssword=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the AS400 server is running.
subnet	The subnet mask value
pollInterval	The polling interval for the monitor.
os	The operating system of the server. Value is 'AS400/iSeries'.
username	The username of the AS400/iSeries server.
password	The password of the AS400/iSeries server.

Sample Request:

```
http://prod-server2:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5&type=servers
&displayname=apmas400&host=pub1.rzkh.de&subnet=255.255.255.0&pollInterval=5
&os=AS400/iSeries&username=nimda&password=admin
```

FreeBSD

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]&host=[HOST]
&subnet=[SUBNET]&pollInterval=[POLLINTERVAL]&os=[OS]&username=[USERNAME]&pa
ssword=[PASSWORD]
&mode=[MODE]&snmptelnetport=[SNMPTELNETPORT]&prompt=[PROMPT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the FreeBSD server is running.
subnet	The subnet mask value
pollInterval	The polling interval for the monitor.
os	The operating system of the server. Value is 'FreeBSD'.
username	The username of the FreeBSD server.
password	The password of the FreeBSD server.
mode	The mode of monitoring. Value is TELNET
snmptelnetport	The port where Telnet service is running. Default value is 23.
prompt	The command prompt value. Value is \$.

Sample Request:

```
http://prod-server4:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db9028
2f5
&type=servers&displayname=apmfreebsd&host=cm-
bsd&subnet=255.255.255.0&pollInterval=5&os=FreeBSD&username=test&password=t
est
&mode=TELNET&snmptelnetport=23&prompt=$
```

HP-UX

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&username=[USERNAME]&password=[PASSWORD]&os=[OS]
&mode=[MODE]&snmptelnetport=[SNMPTELNETPORT]&host=[HOST]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
username	The username of the HP-UX server.
password	The password of the HP-UX server.
os	The operating system of the server. Value is 'HP-UX'.
mode	The mode of monitoring. Values are SSH or TELNET
snmptelnetport	The port where SSH/Telnet service is running. Default values are 23 (for Telnet) and 22 (for SSH).
host	The name of the host where the HP-UX server is running.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db9028
2f5&type=servers
&displayname=apmhpux&username=test&password=test&os=HP-
UX&mode=SSH&snmptelnetport=22&host=hpuxtests
```

Linux

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&snmptelnetport=[SNMPTELNETPORT]&os=[OS]&mode=[MODE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the Linux server is running.
snmptelnetport	The port where SSH/Telnet/SNMP is running. Default values are 23 (for Telnet), 22 (for SSH) and 161 (for SNMP).
os	The operating system of the server. Value is 'Linux'.
mode	The mode of monitoring. Value is either SNMP, SSH or TELNET.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5&type=servers&displayname=apmlinux&host=shakthiprian&snmptelnetport=161&os=Linux&mode=SNMP
```

Mac OS**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&snmptelnetport=[SNMPTELNETPORT]&os=[OS]&mode=[MODE]&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the Mac OS is running.
snmptelnetport	The port where SSH/Telnet/SNMP is running. Default values are 23 (for Telnet), 22 (for SSH) and 161 (for SNMP).
os	The operating system of the server. Value is 'Mac OS'.
mode	The mode of monitoring. Value is either SNMP, SSH or TELNET.

Field	Description
username	The user name of the Mac OS server.
password	The password of the Mac OS server.

Sample Request:

```
http://prod-server3:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=servers&displayname=apmmac&host=apptest-mac&snmpnetport=23&os=Mac
OS&mode=TELNET
&username=administrator&password=vembu
```

Novell**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&snmpnetport=[SNMPNETPORT]&os=[OS]&mode=[MODE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the Novell server is running.
snmpnetport	The port where SNMP is running. Default value is 161.
os	The operating system of the server. Value is 'Novell'.
mode	The mode of monitoring specified for the server. Value is 'SNMP'.

Sample Request:

```
http://production-server2:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=servers&displayname=apmnovell&host=smrithil&snmpnetport=161&os=Nov
ell&mode=SNMP
```

Sun Solaris

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&snmptelnetport=[SNMPTELNETPORT]&os=[OS]&mode=[MODE]&username=[
USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the Sun Solaris server is running.
snmptelnetport	The port where SSH/Telnet/SNMP is running. Default values are 23 (for Telnet), 22 (for SSH) and 161 (for SNMP).
os	The operating system of the server. Value is 'SUN'.
mode	The mode of monitoring specified for the server. Value should be either SNMP, TELNET or SSH.
username	The user name of the Sun Solaris server.
password	The password of the Sun Solaris server.

Sample Request:

```
http://prod-server7:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db9028
2f5
&type=servers&displayname=apmsolaris&host=cagent-
solaris2&snmptelnetport=23&os=SUN&mode=TELNET&username=guest&password=guest
```

Windows

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&snmptelnetport=[SNMPTELNETPORT]&os=[OS]&mode=[MODE]&username=[
USERNAME]&password=[PASSWORD]
```


Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The category type of the monitor you want to add. Value should be 'servers'.
host	The name of the host where the Windows server is running.
snmpTelnetport	The port where SNMP is running. Default value is 161.
os	The operating system of the server. Values can be Windows 2000, Windows 2003, Windows XP, WindowsNT, Windows Vista or Windows 2008.
mode	The mode of monitoring specified for the server. Value is 'SNMP'.
username	The user name of the Windows server.
password	The password of the Windows server.

Sample Request:**To add Windows server in SNMP mode:**

```
http://prod-server6:8080/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=servers&displayname=apmwindows&host=app-xp5&os=Windows
XP&mode=SNMP&snmpTelnetport=161&snmpCommunityString=public
```

To add Windows server in WMI mode:

```
http://prod-server6:8080/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=servers&displayname=apmwindows&host=app-xp5&snmpTelnetport=161&os=Windows
XP&mode=SNMP&username=administrator&password=vembu
```

AddMonitor API - Database Servers

This section explains how to use the AddMonitor API to add monitors of the category type 'Database Servers'. The following databases are supported:

- IBM DB2
- Memcached
- MS SQL
- MySQL
- Oracle
- PostgreSQL
- Sybase

IBM DB2

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&username=[USERNAME]&host=[HOST]&password=[PASSWORD]&port=[PORT]&instance=[
INSTANCE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be db2.
username	The user name of the user who has permission to access the DB2 database.
host	The name of the host in which DB2 is running.
password	The password of the user who has permission to access the DB2 database.
port	The port number where DB2 is running.
instance	The database/instance name.

Sample Request:

```
http://prod-server1:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db9028
```

2f5

&type=db2&displayname=appmanagerdb2&username=db2admin&host=app-
xp4&password=admin&port=50000&instance=SAMPLEDB

Memcached

Syntax:

http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&Transaction=[TRANSACTION
]

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be Memcached.
host	The name of the host in which Memcached server is running.
port	The port number where Memcached server is running.
Transaction	Denotes if transaction test is enabled or not. Value should be either yes or no

Sample Request:

http://prod-server4:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=Memcached&displayname=mem_test&host=app-linux2&port=11211&Transaction=yes

MS SQL

Syntax:

http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&username=[USERNAME]&host=[HOST]&password=[PASSWORD]&port=[PORT]&instance=[
INSTANCE]&authentication=[AUTHENTICATION]

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be ms sql.
username	The name of the user who has permission to access the MS SQL server.
host	The name of the host in which MS SQL is running.
password	The password of the user who has permission to access the MS SQL server.
port	The port number where MS SQL is running.
instance	The database/instance name. This is optional field.
authentication	The authentication type. Value should be either SQL or Windows.

Sample Request:

```
http://prod-server7:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=ms_sql&displayname=appmanagemssql&username=sa&host=app-
xp2&password=Advent1&port=1433&instance=&authentication=SQL
```

MySQL**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&username=[USERNAME]&host=[HOST]&password=[PASSWORD]&port=[PORT]&instance=[
INSTANCE]&authentication=[AUTHENTICATION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be mysql.
username	The name of the user who has permission to access the MySQL server.
host	The name of the host in which MySQL is running.
password	The password of the user who has permission to access the MySQL server.
port	The port number where MySQL is running.

Field	Description
instance	The database/instance name. This is optional field.
authentication	The authentication type. Value should be SQL

Sample Request:

```
http://prod-server3:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=mysql&displayname=appmanagemysql&username=root&host=shakthiprian&password=appmanager&port=13329&instance=mysql&authentication=SQL
```

Oracle**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&username=[USERNAME]&host=[HOST]&password=[PASSWORD]&port=[PORT]&instance=[
INSTANCE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be oracle.
username	The name of the user who has permission to access the Oracle database.
host	The name of the host in which Oracle is running.
password	The password of the user who has permission to access the Oracle database.
port	The port number where Oracle is running.
instance	The database/instance name. This is optional field.

Sample Request:

```
http://prod-server7:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5
&type=oracle&displayname=appmanageroracle&username=rajesh&host=swissql-xpl&password=rajesh&port=1521&instance=orcl
```

PostgreSQL

Syntax:

`http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&instance=[INSTANCE]`

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be PostgreSQL.
host	The name of the host in which PostgreSQL is running.
port	The port number where PostgreSQL is running.
username	The name of the user who has permission to access the PostgreSQL database.
password	The password of the user who has permission to access the PostgreSQL database.
instance	The database/instance name. This is optional field.

Sample Request:

`http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98&type=PostgreSQL&displayname=postSQL&host=app-xp2&port=5432&username=postgres&password=postgres&instance=postgres`

Sybase

Syntax:

`http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&username=[USERNAME]&host=[HOST]&password=[PASSWORD]&port=[PORT]&instance=[INSTANCE]`

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the database you want to add. Value should be sybase.
host	The name of the host in which Sybase is running.
port	The port number where Sybase is running.
username	The name of the user who has permission to access the Sybase database.
password	The password of the user who has permission to access the Sybase database.
instance	The database/instance name. This is optional field.

Sample Request:

```
http://prod-server3:9090/AppManager/xml/AddMonitor?apikey=5bc6a8e9a30d5bf894586d4db90282f5&type=sybase&displayname=appmanagersybase&username=sa&host=app-xp3&password=&port=5000&instance=master
```

AddMonitor API - Services

This section explains how to use the AddMonitor API to add monitors of the category type 'Services'.

The following services are supported:

- Active Directory
- DNS Monitor
- FTP/SFTP Monitor
- JMX Applications
- LDAP Server
- Ping Monitor
- Service Monitoring
- SNMP/Network Device
- Telnet

Active Directory

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'ActiveDirectory'.
host	The name of the host in which the Active Directory service is running.
username	The Active Directory username.
password	The Active Directory password.

Sample Request:

```
http://operation-server3:9099/AppManager/xml/AddMonitor?apikey=123b7328e4b41d1efe64aa7980d83d77&type=ActiveDirectory&displayname=active_mon&host=app-xp4&username=administrator&password=vembu
```


DNS Monitor

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&timeout=[TIMEOUT]&SearchField=[SEARCHFIELD]
&TargetAddress=[TARGETADDRESS]&LookupAddress=[LOOKUPADDRESS]&RecordType=[RECORDTYPE]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'DNSMonitor'.
displayname	The display name of the host in which the monitor is running.
timeout	The timeout value in seconds.
SearchField	The value of SearchField. Options include None, Record Name, Address, Additional Name, Target, Admin, Host, Alias, Port and Priority.
TargetAddress	Host Name / IP Address to connect to the service
LookupAddress	The address you want to check in the DNS Server.
RecordType	The expected record type returned for the lookup address. The options include A, AAAA, CNAME, MX, NS, PTR, SOA, SPF, SRV and TXT.

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=DNSMonitor&displayname=dnstttttt&timeout=15&SearchField=Record Name
&TargetAddress=192.168.4.121&LookupAddress=appmanager.com&RecordType=A
```

FTP/SFTP Monitor

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]
&TargetAddress=[TARGETADDRESS]&DownloadFile=[DOWNLOADFILE]
&IsSecured=[ISSECURED]&UploadFile=[UPLOADFILE]&RemoteSourceFileName=[REMOTE
SOURCEFILENAME]
&RemoteDestinationFileName=[REMOTEDESTINATIONFILENAME]&LocalSourceFileName=[
LOCALSOURCEFILENAME]
&LocalDestinationFileName=[LOCALDESTINATIONFILENAME]&timeout=[TIMEOUT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'FTPMonitor'.
port	The port number where the FTP/SFTP service is running.
username	The FTP/SFTP user name.
password	The FTP/SFTP password.
TargetAddress	Host Name / IP Address to connect to the service.
DownloadFile	Indicates if download is enabled. Possible values include yes and no. If you would like to monitor the downloads (mget) through FTP/SFTP while simulateneously downloading the file, specify yes.
IsSecured	Specifies if the connection is secure or not. Value is either yes or no.
UploadFile	Indicates if upload file option is enabled. Values include yes and no. If you would like to upload a file to target address, specify yes.
RemoteSourceFileName	The Remote Source FileName located in the target address. This is applicable only if the value of 'DownloadFile' option is specified as yes.
RemoteDestinationFileName	The Remote Destination FileName located in the target address. This is applicable only if the value of 'UploadFile' option is specified as yes.
LocalSourceFileName	The name of the local source file with full path. The file must be available where Applications Manager instance is running. This is applicable only if the value of 'UploadFile' option is specified as yes.
LocalDestinationFileName	The local destination FileName with full path. The file will download in the given path where Applications Manager instance is running. This field is applicable only if the value of 'DownloadFile' option is specified as yes
timeout	The timeout value in seconds.

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=FTPMonitor&displayname=ladpapitestooooo&port=22&username=sprasadh&password=sprasadh
&TargetAddress=sprasadh&DownloadFile=no&IsSecured=yes&UploadFile=no
&RemoteSourceFileName=&RemoteDestinationFileName=&LocalSourceFileName=&LocalDestinationFileName=&timeout=15
```

JMX Applications**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&jndiurl=[JNDIURL]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'JMX Applications'.
host	The name of the host in which the monitor is running.
port	The port number where the RMI adapter is running.
jndiurl	The JNDI name. Example:/jmxrmi

Sample Request:

```
http://prod-server1:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=JMX Applications&displayname=apmjmxapp&host=app-xp2&port=1099&jndiurl=/jmxrmi
```

LDAP Server**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&username=[USERNAME]&timeout=[TIMEOUT]&LDAPServer=[LDAPSERVER]
&LDAPServerPort=[LDAPSERVERPORT]&MatchingAttribute=[MATCHINGATTRIBUTE]&FilterCondition=[FILTERCONDITION]
```

`&IsSecured=[ISSECURED]&SearchFilter=[SEARCHFILTER]&SearchResult=[SEARCHRESULT]&SearchBase=[SEARCHBASE]&password=[PASSWORD]`

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'LDAP Server'.
username	The user name of the LDAP server.
timeout	The timeout value in seconds.
LDAPServer	The name of the LDAP Server.
LDAPServerPort	The port at which the LDAP server is running.
MatchingAttribute	The matching attribute value. Values include cn, uid, sn, displayname, givenname, objectclass, dc and ou
FilterCondition	The value of filter condition. Values include equals, contains and notequals
IsSecured	Specifies if the connection is secure or not. Value is either yes or no.
SearchFilter	The value of Search Filter. This field is optional.
SearchResult	The string value that matches with search results.
SearchBase	The value of SearchBase. This is mandatory field when adding a LDAP monitor.
password	The password of the LDAP server.

Sample Request:

```
http://operations-server9:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=LDAP
Server&displayname=ldap_serverqqqq&username=cn=administrator,cn=users,dc=pm
p,dc=com
&timeout=10&LDAPServer=pmp-
2k8s&LDAPServerPort=389&MatchingAttribute=cn&FilterCondition=equals&IsSecur
ed=no
&SearchFilter=&SearchResult=&SearchBase=&Password=Vembul23
```

Ping Monitor

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&timeout=[TIMEOUT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'Ping Monitor'.
host	The host in which the monitor is running.
timeout	The timeout value in seconds.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=Ping Monitor&displayname=apmping&host=smrithil&timeout=5
```

Service Monitoring

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be service.
host	The host in which the monitor is running.
port	The port number in which the service is running.

Sample Request:

```
http://prod-server3:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98&type=service&displayname=apmservice&host=smrithil&port=9090
```

SNMP/Network Device**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&snmpCommunityString=[SNMPCOMMUNITYSTRING]&timeout=[TIMEOUT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be SNMP / Network Device.
host	The host in which the monitor is running.
port	The port number in which SNMP is running.
snmpCommunityString	The SNMP community string value. Default value is public.
timeout	The timeout value in seconds.

Sample Request:

```
http://prod-server4:9099/AppManager/xml/AddMonitor?apikey=c9684ec1361be61f48cd1bd2221ac3fc&type=SNMP/Network Device&displayname=apmsnmp&host=sprasadh&port=161&snmpCommunityString=public&timeout=5
```

Telnet**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be telnet.
host	The host name in which the monitor is running.
port	The port number in which Telnet is running.

Sample Request:

```
http://operation-  
server2:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3  
f98  
&type=telnet&displayname=apmtelnet&host=smrithil&port=23
```

AddMonitor API - Web Server/Services

This section explains how to use the AddMonitor API to add monitors of the category type 'Web Server/Services'. The following monitors are supported:

- Apache Server
- IIS Server
- PHP
- Real Browser Monitor (RBM)
- Web Server

Apache Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&serverstatusurl=[SERVERSTATUSURL]&apacheurl=[APACHEURL]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Apache Server.
host	The name of the host where the Apache server is running.
port	The port number where the Apache server is running.
apacheauth	Denotes whether the Apache server is authenticated. Possible values are true and false.
apacheUserName	The user name of the Apache server. This is required only if apacheauth value is true.
apachepassword	The password of the Apache server. This is required only if apacheauth value is true.
sslenabled	Indicates whether SSL is enabled. The value should be either on or off
serverstatusurl	Indicates whether the Apache Server Status url can be modified. The value should be either true or false.
apacheurl	The Apache server status url. Example: http://<host-name:portNumber>server-status?auto

Sample Request:

```
http://prod-
server5:9090/AppManager/xml/AddMonitor?apikey=256d041620d0aee9901558b44706d
c84
&type=Apache
Server&displayname=apmapache&host=shakthiprian&port=8080&serverstatusurl=tr
ue&apacheurl=ddss
```

IIS Server**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be IIS Server.
host	The name of the host where the IIS is running.
port	The port number where the IIS is running.

Sample Request:

```
http://prod-
server8:9091/AppManager/xml/AddMonitor?apikey=90c166a4646e29315a57ecald6b88
858
&type=IIS Server&displayname=apmiis&host=app-xp2&port=80
```

PHP**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&serverpath=[SERVERPATH]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be PHP.
host	The name of the host where the PHP is running.
port	The port number where the PHP is running.
serverpath	The path to be used for connection. The default value is /phpstats.php

Sample Request:

```
http://operation-
server9:9091/AppManager/xml/AddMonitor?apikey=90c166a4646e29315a57eca1d6b88
858
&type=PHP&displayname=apmiis&host=myesuraj&port=80&serverpath=/phpstats.php
```

Real Browser Monitor (RBM)**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&rbmagentID=[RBMAGENTID]&timeout=[TIMEOUT]&script
name=[SCRIPTNAME]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be RBM.
rbmagentID	The ID of the RBM agent.
timeout	The timeout value in seconds.
scriptname	The name of the web script.

Sample Request:

```
http://prod-
server8:9091/AppManager/xml/AddMonitor?apikey=90c166a4646e29315a57eca1d6b88
858
&type=RBM&displayname=RBM_test&rbmagentID=10000000&timeout=15&scriptname=ne
ws
```

Web Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Web Server.
host	The name of the host where the web server is running.
port	The port number where the web server is running.

Sample Request:

```
http://prod-server8:9091/AppManager/xml/AddMonitor?apikey=90c166a4646e29315a57ecald6b88
858
&type=Web Server&displayname=apmweb&host=app-xp2&port=80
```

AddMonitor API - Mail Servers

This section explains how to use the AddMonitor API to add monitors of the category type 'Mail Server'. The following monitors are supported:

- Exchange Server
- Mail Server

Exchange Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&version=[V
ERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the mail server you want to add. Value should be Exchange Server.
host	The name of the host where the Exchange server is running.
port	The port number where the Exchange server is running.
username	The user name for the system in which Exchange server is running.
password	The password for the system in which Exchange server is running.
version	The Exchange server version. Supported versions are 2000, 2003, 2007, 2010 and 5.

Sample Request:

```
http://prod-server6:9090/AppManager/xml/AddMonitor?apikey=2712f158d675135e9b3d81d9efd53
3c0
&type=Exchange Server&displayname=apmexchange&host=emp-
ex03&port=25&username=exchange\administrator&password=vembu&version=2003
```

Mail Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&version=[V
ERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Mail Server.
host	The name of the host where the mail server is running.
port	The SMTP port number
emailid	An email id available in the mail server.
timeout	The time out value in seconds.
mailMsg	The message to appear in the subject of the email.

Sample Request:

```
http://prod-server5:9098/AppManager/xml/AddMonitor?apikey=4c362569ccc528be78fafdcc2317b
c5c
&type=Mail
Server&host=smtp&displayname=apmmail&port=25&emailid=myesura@zohocorp.com&t
imeout=15&mailMsg=Testing mail server.
```

AddMonitor API - Middleware/Portal

This section explains how to use the AddMonitor API to add monitors of the category type 'Middleware/Portal'. The following monitors are supported:

- MS Office SharePoint
- WebLogic Integration
- IBM WebSphere MQ
- Microsoft Message Queue (MSMQ)

MS Office SharePoint

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be MSOfficeSharePointServer.
host	The name of the host where the Office SharePoint server is running.
username	The user name of the SharePoint server .
password	The password of the SharePoint server.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=4df5040d6db873dcda4359b259fd494&type=MSOfficeSharePointServer&displayname=ms&host=app-xp3&username=administrator&password=vembu
```

WebLogic Integration

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&version=[VERSION]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be WebLogic Integration.
host	The name of the host where the WebLogic Integration server is running.
port	The port number where the WebLogic Integration server is running.
username	The user name of the WebLogic Integration server .
password	The password of the WebLogic Integration server.
version	The WebLogic Integration server version. Value is 8.1

Sample Request:

```
http://prod-server3:9090/AppManager/xml/AddMonitor?apikey=136edbeb3ccb83c6cc71df03ef273313
&type=WebLogic Integration&displayname=apm&host=app-linux1&port=7001&username=weblogics&password=weblogic&version=8.1
```

IBM WebSphere MQ**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&listenerport=[PORT]&displayname=[USERNAME]&serverconnectionchannel=[SERVERCONNECTIONCHANNEL]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be IBM WebSphere MQ.
host	The name of the host where the WebSphere MQ server is running.
listenerport	The listener port number of the IBM WebSphere MQ server.

Field	Description
displayname	The display name of the monitor.
serverconnectionchannel	The server connection channel through which the WebSphere MQ clients communicate.

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=256d041620d0aee9901558b44706dc84
&type=IBM Websphere MQ&host=app-xp4&listenerport=1414&displayname=mqws&serverconnectionchannel=c1
```

Microsoft Message Queue (MSMQ)**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Microsoft MQ.
host	The name of the host where the Microsoft MQ server is running.
username	The username of the MSMQ server
password	The password of the MSMQ server

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=256d041620d0aee9901558b44706dc84
&type=Microsoft MQ&displayname=msmq&host=app-server&username=administrator&password=password
```


AddMonitor API - Custom Monitors

This section explains how to use the AddMonitor API to add monitors of the category type 'Custom Monitors'. The following monitors are supported:

- Windows Performance Counters
- Database Query Monitor

Windows Performance Counters

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&username=[USERNAME]&password=[PASSWORD]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Windows Performance Counters.
host	The name of the host where the Windows Performance Counters is running.
username	The user name of the host running Windows Performance Counters.
password	The password of the host running Windows Performance Counters.

Sample Request:

```
http://app-xp4:9090/AppManager/xml/AddMonitor?apikey=ee8d8e237bd5e1a0d8aed16a381c3b73&type=Windows Performance Counters&host=app-xpml1&displayname=hhhh&username=asasaa&password=vembu
```

Database Query Monitor

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]&databasetype=[DATABASETYPE]&databasename=[DATABASENAME]&showqueryoutput=[S
```

```
HOWQUERYOUTPUT]
&queries=[QUERIES]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be QueryMonitor.
host	The name of the host where the database server is running.
port	The port number where the database is running
username	The user name of the database server .
password	The password of the database server.
databasetype	The database type for which the query is executed.
databasename	The name of the database server.
showqueryoutput	Option to specify whether you prefer query output. Values are yes and no
queries	Denotes the database query. There can be a maximum of five queries.

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=bbab7f01458e96595b06d5c27efcc3af
&type=QueryMonitor&displayname=query&host=app-
xp2&port=1433&username=sa&password=Advent1&databasetype=MsSQL&databasename=
AMDB&showqueryoutput=yes&queries=select * from user
```

AddMonitor API - Virtualization

This section explains how to use the AddMonitor API to add monitors of the category type 'Virtualization'. The following monitors are supported:

- VMware ESX/ESXi Server
- Microsoft Hyper-V Server

VMware ESX/ESXi Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&host=[HOST]&port=[PORT]&username=[USERNAME]&password=[PASSWORD]
&addtoGroup=[ADDTOGROUP]&groupID=[GROUPID]&monitorvms=[MONITORVMS]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be VMware ESX/ESXi.
host	The name of the host where the VMWare ESX/ESXi server is running.
port	The port number where the VMware ESX/ESXi server is running.
username	The user name of the VMware ESX/ESXi server.
password	The password of the VMware ESX/ESXi server.
addtoGroup	Denotes if the monitor should be added to monitor group. Value is either true or false.
groupID	The monitor group ID
monitorvms	Indicates the way the virtual machines of the ESX server are to be monitored. Possible values are no, yes and onlyavailability. The value no means the VMs will not be discovered. The value yes indicates that the VMs will be discovered and monitored. The value onlyavailability indicates that the VMs will be discovered but the metrics will not be monitored (will not count for licensing).

Sample Request:

```
http://prod-
server5:9098/AppManager/xml/AddMonitor?apikey=e249ce592ad1052c4ea605bcf3125
ad9
&type=VMWare ESX/ESXi&displayname=vnwgroup&host=esx-
2&port=443&username=root&password=password&addToGroup=true
&groupID=10000024&monitorvms=onlyavailability
```

Microsoft Hyper-V Server**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&host=[HOST]&port=[PORT]&displayname=[DISPLAYNAME]&password=[PASSWORD]
&addvms=[ADDVMS]&username=[USERNAME]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Hyper-V Server.
host	The name of the host where the Hyper-V server is running.
port	The port number where the Hyper-V server is running.
password	The password of the Hyper-V server.
addvms	Denotes whether the performance metrics of VMs should be collected. Value is either yes or no
username	The user name of the Hyper-V server.

Sample Request:

```
http://prod-
server6:9090/AppManager/xml/AddMonitor?apikey=256d041620d0aee9901558b44706d
c84
&type=Hyper-V Server&host=amp-w2k8-
64&port=8080&displayname=apmhyperv&password=Vembul23app2
&addvms=yes&username=administrator
```

AddMonitor API - Cloud Apps

This section explains how to use the AddMonitor API to add monitors of the category type 'Virtualization'. The following monitors are supported:

- Amazon

Amazon

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&accessKey=[ACCESSKEY]&SecretAccessKey=[SECRETACCESSKEY]&displayname=[DISPL
AYNAME]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be Amazon
accessKey	The Access Key Id of the AWS for accessing the AWS through the API.
SecretAccessKey	The secret access key of the AWS.

Sample Request:

```
http://prod-server2:9098/AppManager/xml/AddMonitor?apikey=4c362569ccc528be78fafdcc2317b
c5c
&type=Amazon&accessKey=19879sd&SecretAccessKey=2dhsoid&displayname=amazon
monitor
```

AddMonitor API - EUM Monitors

This section explains how to use the AddMonitor API to add monitors of the category type End User Monitoring (EUM). The following monitors are supported:

- Ping
- DNS
- LDAP Server
- Mail Server
- Real Browser Monitor

The following parameters are common in API requests for EUM monitors:

Field	Description
eumAgents	The display name(s) of the EUM agent(s). If there are multiple entries, they can be comma separated.
eumAgentsId	The unique ID of the EUM agents configured. These can be specified as comma separated.
runOnServer	Specifies if the monitor has to be created in Applications Manager. Possible values are 'True' or 'False'

Note:

- 1) It is not mandatory to use both 'eumAgents' and 'eumAgentsId' parameters in the same API request. You can use either one of these.
- 2) The runOnServer parameter is not applicable for Real Browser Monitor (RBM)

Ping

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
displayname=[DISPLAYNAME]
&host=[HOST]&timeout=[TIMEOUT]&eumAgents=[EUMAGENTS]&eumAgentsId=[EUMAGENTI
D]&runOnServer=[RUNONSERVER]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'Ping Monitor'.
host	The host in which the monitor is running.
timeout	The timeout value in seconds.

Sample Request:

```
http://prod-server5:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=Ping
Monitor&displayname=apmping&host=smrithil&timeout=5&eumAgents=eumflorida&runOnServer=True
```

DNS**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&timeout=[TIMEOUT]&SearchField=[SEARCHFIELD]
&TargetAddress=[TARGETADDRESS]&LookupAddress=[LOOKUPADDRESS]&RecordType=[RECORDTYPE]
&eumAgents=[EUMAGENTS]&eumAgentsId=[EUMAGENTID]&runOnServer=[RUNONSERVER]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'DNSMonitor'.
displayname	The display name of the host in which the monitor is running.
timeout	The timeout value in seconds.
SearchField	The value of SearchField. Options include None, Record Name, Address, Additional Name, Target, Admin, Host, Alias, Port and Priority.
TargetAddress	Host Name / IP Address to connect to the service
LookupAddress	The address you want to check in the DNS Server.
RecordType	The expected record type returned for the lookup address. The options include A, AAAA, CNAME, MX, NS, PTR, SOA, SPF, SRV and TXT.

Sample Request:

```
http://prod-server8:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=DNSMonitor&displayname=dnstttttt&timeout=15&SearchField=Record Name
&TargetAddress=192.168.4.121&LookupAddress=appmanager.com&RecordType=A&eumAgents=eumbel
&runOnServer=True
```

LDAP Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&username=[USERNAME]&timeout=[TIMEOUT]&LDAPServer
=[LDAPSERVER]
&LDAPServerPort=[LDAPSERVERPORT]&MatchingAttribute=[MATCHINGATTRIBUTE]&FilterCondition=[FILTERCONDITION]
&IsSecured=[ISSECURED]&SearchFilter=[SEARCHFILTER]&SearchResult=[SEARCHRESULT]&SearchBase=[SEARCHBASE]&password=[PASSWORD]
&eumAgents=[EUMAGENTS]&eumAgentsId=[EUMAGENTID]&runOnServer=[RUNONSERVER]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'LDAP Server'.
username	The user name of the LDAP server.
timeout	The timeout value in seconds.
LDAPServer	The name of the LDAP Server.
LDAPServerPort	The port at which the LDAP server is running.
MatchingAttribute	The matching attribute value. Values include cn, uid, sn, displayname, givenname, objectclass, dc and ou
FilterCondition	The value of filter condition. Values include equals, contains and notequals
IsSecured	Specifies if the connection is secure or not. Value is either yes or no.
SearchFilter	The value of Search Filter. This field is optional.
SearchResult	The string value that matches with search results.
SearchBase	The value of SearchBase. This is mandatory field when adding a LDAP monitor.
password	The password of the LDAP server.

Sample Request:

```
http://operations-server9:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
```



```
&type=LDAP
Server&displayname=ldap_serverqqqq&username=cn=administrator,cn=users,dc=pm
p,dc=com
&timeout=10&LDAPServer=pmp-
2k8s&LDAPServerPort=389&MatchingAttribute=cn&FilterCondition>equals&IsSecur
ed=no
&SearchFilter=&SearchResult=&SearchBase=&Password=Vembul23&eumAgents=eumbel
&runOnServer=True
```

Mail Server

Syntax:

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]&
host=[HOST]&port=[PORT]
&displayname=[DISPLAYNAME]&emailid=[EMAILID]&timeout=[TIMEOUT]&authRequired
=[AUTHREQUIRED]
&sslEnabled=[SSEENABLED]&username=[USERNAME]&password=[PASSWORD]&tlsEnabled
=[TLSEENABLED]
&pollinterval=[POLLINTERVAL]&mailsubject=[MAILSUBJECT]&fetchEnabled=[FETCHE
NABLED]&fetchType=[FETCHTYPE]
&fsHost=[FSHOST]&fsport=[FSPORT]&fsSSLEnabled=[FSSSEENABLED]&fsTLSEnabled=[
FSTLSEENABLED]
&fsUserName=[FSUSERNAME]&fsPassword=[FSPASSWORD]&eumAgents=[EUMAGENTS]&eumA
gentsId=[EUMAGENTID]&runOnServer=[RUNONSERVER]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the service you want to add. Value should be 'Mail Server'.
host	The SMTP host name
port	The port at which SMTP is running.
emailid	The email address to which the mail will be sent.
timeout	The timeout value in seconds.
authRequired	Indicates if the SMTP requires authentication. Values are 'Yes' or 'No'
sslEnabled	Indicates if the SMTP host should be accessed through SSL. Values are 'Yes' or 'No'
username	The username of the SMTP host
password	The password of the SMTP host
tlsEnabled	Denotes whether TLS should be used for SMTP

Field	Description
pollinterval	The polling interval of the monitor in seconds.
mailSubject	The message to appear in the subject of the email.
fetchEnabled	Indicates if the POP/IMAP server should be monitored. Values are 'Yes' or 'No'.
fetchType	Indicates the service that is monitored. If you want to add POP type, specify the value as 1. If you want to monitor IMAP server, specify the value as 2.
fsHost	The host name of the POP/IMAP server
fsport	The port at which the POP/IMAP server is running.
fsSSEnabled	Indicates whether the POP/IMAP server is SSL enabled or not. Values are 'Yes' or 'No'.
fsTLSEnabled	Indicates whether TLS should be used for POP/IMAP. Values are 'Yes' or 'No'.
fsUserName	The user name of the POP/IMAP server.
fsPassword	The password of the POP/IMAP server

Sample Request:

```
http://operations-server9:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98
&type=Mail
Server&host=smtpl&port=23&displayname=apmsmtpl&emailid=admin@yourdomain.com&
timeout=5&authRequired=Yes
&sslEnabled=Yes&username=guest&password=guest&tlsEnabled=Yes&pollinterval=6
0&mailsubject=Testing Mail Server
&fetchEnabled=Yes&fetchType=1&fsHost=POP1&fsport=110&fsSSEnabled=Yes&fsTLS
Enabled=Yes&fsUserName=admin&fsPassword=Vembul23
&eumAgents=euml&runOnServer=True
```

Real Browser Monitor**Syntax:**

```
http://[Host]:[Port]/AppManager/xml/AddMonitor?apikey=[APIKEY]&type=[TYPE]
&displayname=[DISPLAYNAME]&scriptname=[SCRIPTNAME]&pollinterval=[POLLINTERV
AL]&timeout=[TIMEOUT]
&eumAgents=[EUMAGENTS]&eumAgentsId=[EUMAGENTID]
```

Request Parameters:

The parameters involved in the API request are described below. Also, refer the list of common Request Parameters.

Field	Description
type	The type of the monitor you want to add. Value should be 'RBM'.
scriptname	The script name for RBM
pollinterval	The polling interval for the monitor in seconds
timeout	The time out value in seconds.

Sample Request:

```
http://operations-server9:9090/AppManager/xml/AddMonitor?apikey=40648ef160f4786b20ed89ea51aa3f98&type=RBM&displayname=rbml&scriptname=script1&pollinterval=60&timeout=30&eu  
mAgents=euml
```

ListUserDetails API

This API is used to get user details such as the role of the user and username of the user.

Sample Request

http://[Host]:[Port]/AppManager/xml/ListUserDetails?apikey=[APIKEY]

Request Parameters

The parameters involved in executing this API request are:

Field	Description
apikey	The key generated using the Generate API Key option in the 'Admin' tab.

Example

http://app-windows:59090/AppManager/xml/ListUserDetails?apikey=93c6eb60184e41f10fba2f365060b8e3

Example Output:

```
<AppManager-response uri="/AppManager/xml/ListUserDetails">
  <result>
    <response method="ListUserDetails">
      <Users>
        <User UserName="admin" Role="ADMIN"/>
        <User UserName="admin" Role="USERS"/>
        <User UserName="op" Role="OPERATOR"/>
        <User UserName="user" Role="USERS"/>
        <User UserName="man" Role="MANAGER"/>
      </Users>
    </response>
  </result>
</AppManager-response>
```

If the API is not executed correctly, the request will fail and errors will be shown as given below:

```
<AppManager-response uri="/AppManager/xml/ListUserDetails">
  <result>
    <response response-code="4004">
      <message>The specified apikey [ "+apiKey+" ] in the request is invalid. Kindly login to Application Manager and check
for the key in generate key in Admin tab.</message>
    </response>
  </result>
</Apm-response>
```

Refer this page for a list of common error conditions.

PollNow API

This API allows you to poll a particular monitor.

Sample Request

http://[Host]:[Port]/AppManager/xml/PollNow?apikey=[APIKEY]&resourceid=[RESOURCEID]

Request Parameters

The parameters involved in executing this API request are:

Field	Description
apikey	The key generated using the Generate API Key option in the 'Admin' tab.
resourceid	The resource id of the monitor that needs to be polled.

Example

http://app-

xp5:9099/AppManager/xml/PollNow?apikey=123b7328e4b41d1efe64aa7980d83d77&resourceid=10000293

Example Output:

```
<AppManager-response uri="/AppManager/xml/PollNow">
<result>
<response method="PollNow">
<message>The monitor polled successfully.</message>
</response>
</result>
</AppManager-response>
```

If the API is not executed correctly, the request will fail and errors will be shown as given below:

```
<AppManager-response uri="/AppManager/xml/PollNow">
<result>
<response response-code="4037">
<message>Improper resourceid in the request.</message>
</response>
</result>
</Apm-response>
```

Refer this page for a list of common error conditions.

DeleteMonitor API

This API is used to delete a monitor.

Sample Request

http://[Host]:[Port]/AppManager/xml/DeleteMonitor?apikey=[APIKEY]&resourceid=[RESOURCEID]

Request Parameters

The parameters involved in executing this API request are:

Field	Description
apikey	The key generated using the Generate API Key option in the 'Admin' tab.
resourceid	The resource id of the monitor that needs to be deleted.

Example

http://app-

windows:59090/AppManager/xml/DeleteMonitor?apikey=93c6eb60184e41f10fba2f365060b8e3&resourceid=10000032

Example Output:

```
<AppManager-response uri="/AppManager/xml/DeleteMonitor">
  <result>
    <response method="DeleteMonitor">
      <message>The monitor deleted successfully.</message>
    </response>
  </result>
</AppManager-response>
```

If the API is not executed correctly, the request will fail and errors will be shown as given below:

```
<AppManager-response uri="/AppManager/xml/DeleteMonitor">
  <result>
    <response response-code="4004">
      <message>The specified apikey [ "+apiKey+" ] in the request is invalid. Kindly login to Application Manager and check for the key in generate key in Admin tab.</message>
    </response>
  </result>
</Apm-response>
```

Refer this page for a list of common error conditions.

Error Handling

API execution could result in error conditions. In case of an error, the error information would be sent in the response body. The response body will have <error> as the child node along with the appropriate error code.

Error Codes

The list of HTTP error codes are tabulated below:

Code	Description
4000	<Success Message>
4002	The specified resourceid in request URI should be an integer.
4003	The specified resourceid in request URI is wrong.
4004	The specified apikey ["+apiKey+"] in the request is invalid. Kindly log in to Applications Manager and check for the key in generate key in Admin tab.
4005	The specified type in request URI is wrong.
4006	The given ResoureID in the URL is wrong or repeated.
4007	The specified monitorname in request URI is wrong.
4008	The specified request URI is incorrect.
4016	The specified method in request URI is incorrect.
4024	The given taskid in the URL is wrong.
4025	The specified taskname in the URL is already exist or empty.
4032	The specified parameter in request URI is incorrect.
4033	The taskName cannot be empty.
4034	The taskName already exists.
4035	The taskStatus should be either enable or disable.
4036	The taskType should be either group or monitor.
4037	Improper resourceid in the request.
4038	The startTime should be of the format (HH:MM).

Code	Description
4039	The endTime should be of the format (HH:MM).
4040	DestinationAddress DestinationPort GlobalTrap are mandatory for v1 trap
4041	The effectFrom should be of the format (YYYY-MM-DD HH:MM).
4042	Task Method should be any one among Daily,Weekly or Once.
4043	The totalNumber should be between 1 to 7 only.
4044	The customTaskStartTime should be of the format (YYYY-MM-DD HH:MM).
4045	The customTaskEndTime should be a valid date format like (YYYY-MM-DD HH:MM).
4046	The startDay,startTime,endDay,endTime for weekly Maintenance are incorrect.
4048	The given taskid in the URL is not an integer.
4049	The monitor is under maintenance. Try pollnow after maintenance.
4050	The monitor cant be polled when unmanaged.
4064	Kindly buy the License to avail the Applications Manager API's.
4080	DestinationAddress DestinationPort GlobalTrap are mandatory for v2 trap
4128	Server Error while processing the request.
4201	The pollInterval should be a valid whole number.
4202	The type should not be empty.
4203	The groupID should be a valid whole number.
4204	The WSDLUrl should not be empty.
4205	The WSDLUrl should not be empty.
4206	The username and password mentioned in the request URL should not be empty.
4207	The popHost, smtpUserName and smtpPassword mentioned in the request URL should not be empty.
4208	The rbmagentID mentioned in the request URL should not be empty.
4209	The rbmagentID mentioned in the request URL is repeated or invalid.
4210	The scriptname mentioned in the request URL should not be empty.
4211	The displayname mentioned in the request URL should not be empty.

Code	Description
4212	Invalid OS type.
4213	The mode should be any one among SSH/TELNET/SNMP/WMI
4214	The snmptelnetport should be a valid one.
4215	The type mentioned in the request URL is not supported.
4216	The timeout should be a valid one.
4217	The host should not be empty.
4218	The port should be a valid one.
4219	The username mentioned in the request URL should not be empty.
4220	The password mentioned in the request URL should not be empty.
4221	The authentication should SQL or Windows.
4222	The serverpath should not be a empty.
4223	The jndiurl should not be a empty.
4224	The instance should not be a empty.
4225	The Transaction mentioned in the request URL should be yes or no.
4226	The LDAPServer should not be empty.
4227	The LDAPServerPort should not be empty.
4228	The MatchingAttribute should be anyone of cn, uid, sn, displayname, givenname, objectclass, dc, ou.
4229	The FilterCondition should be anyone of equals, contains, notequals.
4230	The IsSecured should be either yes or no.
4231	The TargetAddress mentioned in the request URL should not be empty.
4232	The DownloadFile mentioned in the request URL should not be empty.
4233	The UploadFile should be either yes or no.
4234	The SearchField should not be empty.
4235	The TargetAddress should not be empty.
4236	The LookupAddress should not be empty.

Code	Description
4237	The RecordType should not be empty.
4238	The version of WEBLOGIC should be anyone of 6.1,7.0,8.1,9.x,10.x.
4238	The JNDIPath should not be empty.
4239	The version of JBoss server should be anyone of 3.2.x,4.x,4.0.1,4.0.2 & above,5.0.0 & above.
4240	The version of Tomcat Server should be anyone of 3,4,5,6.
4241	The version of Websphere Server should be anyone of 5.x,6.x,7.x
4242	The mode of Websphere Server should be BASE or ND.
4243	The soapport should be a valid whole number.
4244	The version of Oracle Application Server should be anyone of 10.1.2 or 10.1.3.
4245	The SSL of OracleEBS should be yes or no.
4246	The systemnumber of SAP Server should not be empty.
4247	The logonClient of SAP Server should not be empty.
4248	The language of SAP Server should not be empty.
4249	The specified taskMethod and taskid does not match.
4250	The starttime should less than endtime.
4251	Check for the date time configuration of weekly.
4252	The customTaskStartTime should be less than customTaskEndTime.
4253	The method for UrlMonitor should be post or get.
4254	The httpcondition for UrlMonitor should be as follows. LT for <, GT for >, EQ for =, NE for !=, LE <= and GE for >=.
4255	The url should not be empty.
4256	The version of Exchange Server should be any one of 2007, 2003, 2000, 5.
4257	The databasetype of QueryMonitor should be any one of MySQL, Oracle, DB2, MsSQL, Sybase, Postgres.
4258	The databasetypename of QueryMonitor should not be empty.
4259	The showqueryoutput of QueryMonitor should be any one of yes or no.

Code	Description
4260	The queries of QueryMonitor should not be empty.
4261	The name for adding Monitor Group already exist.
4262	The name should not be empty.
4263	The grouptype should be either monitorgroup or webappgroup.
4264	The userid in the request url is wrong or the values are repeated.
4265	The weblogic.jar is missing and is required for monitoring Weblogic server Version 6.
4266	The weblogic.jar is missing and is required for monitoring Weblogic server Version 7.
4267	The weblogic.jar is missing and is required for monitoring Weblogic server Version 8.
4268	The weblogic.jar is missing and is required for monitoring Weblogic server Version 9.
4269	The weblogic.jar is missing and is required for monitoring Weblogic server Version 10.
4270	The accessKey should not be empty.
4271	The SecretAccessKey should not be empty.
4272	The apacheurl should not be empty.
4273	The serverstatusurl should not be true or false.
4274	The listenerport should not be empty.
4275	The serverconnectionchannel should not be empty.
4444	Error:
4512	The specified time in request URI is incorrect. Either it is more than the current time or not a proper time
4540	This API is not available for Admin Server.

End User Monitoring (EUM)

End User Monitoring (EUM) provides the ability to monitor the health and performance of services from multiple locations outside your corporate firewall. This capability provides you greater visibility into the user experience and behaviors of these services and helps in detecting potential performance problems before end users are affected. It also enables you take steps to improve the user experience of business-critical services.

End user monitoring can be enabled by installing agents in client locations and configuring your monitors to make use of these agents for monitoring. The monitors currently supported by the EUM agent include Ping, DNS, Mail Server, LDAP server and Real Browser Monitor (RBM).

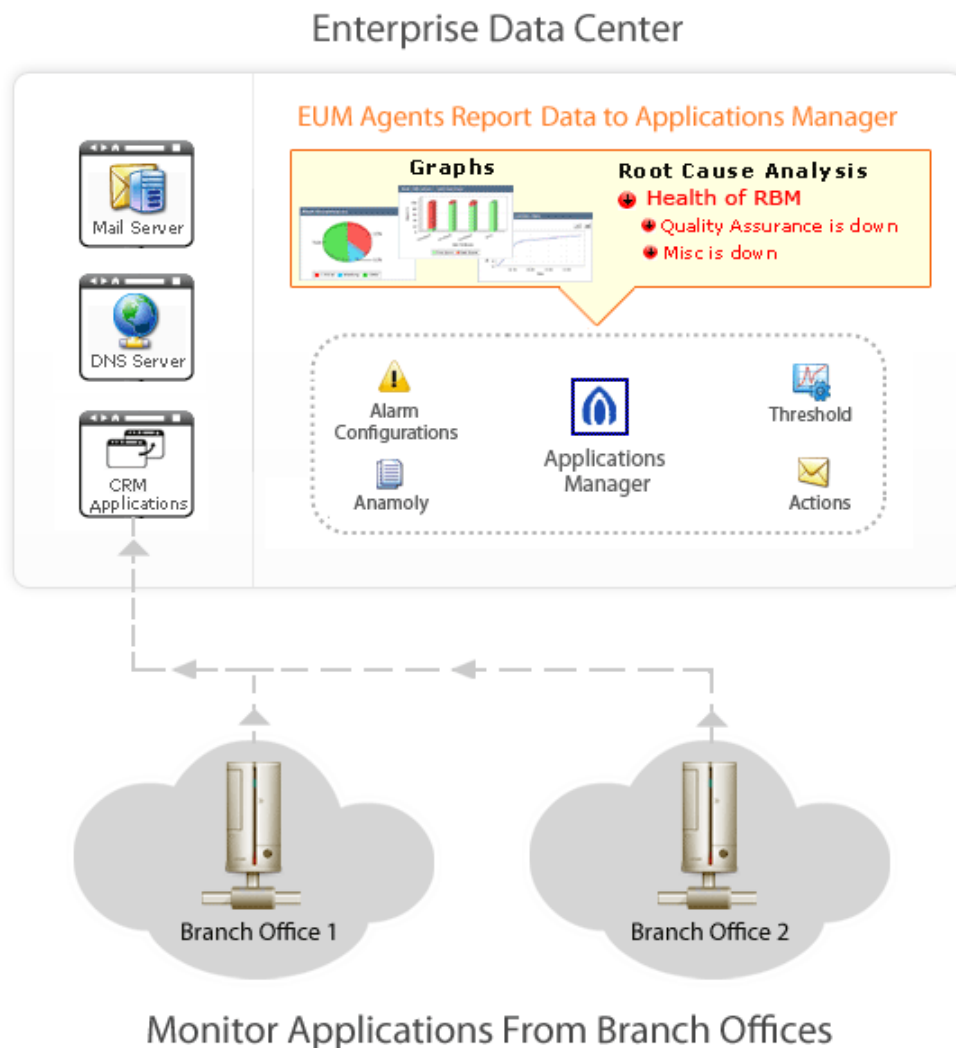
Browse through the following topics to understand EUM better:

- [How does End User Monitoring work?](#)
- [Installing EUM agent](#)
- [EUM Dashboard](#)

How does End User Monitoring (EUM) Work?

End user monitoring enables IT operations ensure that the real end users of an application or service are experiencing good performance. Since the EUM agents take care of collecting and reporting data, the IT administrator is able to accurately keep track of the performance of services without needing to take any additional steps.

To configure EUM monitors, you have to download EUM agents, install them in your branch offices or customer locations, and install Applications Manager server in your head office. Once these agents are enabled, they will collect data about the service performance from these locations and pass it on to the central Applications Manager server. This data will then be processed by Applications Manager and used for measuring the end user experience.



The EUM agents can be installed in multiple branch offices in different cities or in the systems of your end users. All you need is a secure https connection between the agent and the Applications Manager server.

The EUM agent pings the Applications Manager server at specific time intervals and gathers information such as the service configuration details. The service will then be executed from the remote location and the results passed on to the central Applications Manager server. Based on the metrics received from the agent, the Applications Manager server measures the performance of these services and generates performance charts. Some of the performance metrics displayed in the monitor details page include response time from different locations, outage report based on locations, etc.

Based on the information shown in the EUM monitor, the IT team can determine how the service is performing from different locations. If there is a performance issue in a particular agent, they can troubleshoot initiate root cause analysis, isolate the real performance issue and resolve them before end users are affected.

Installing and Uninstalling EUM Agent

This section covers the following topics:

- Installing EUM Agent
 - Windows
 - Linux
- Uninstalling EUM Agent
 - Windows
 - Linux
- End User Monitoring Agent Settings

Installing EUM Agent

To start end user monitoring from multiple locations, you have to install the EUM agents in the respective locations. The agents can be installed in both Windows and Linux systems. Please note that the EUM agents will work only if the central Applications Manager server is running.

Windows

Follow the steps given below to install the EUM agent in Windows systems.

1. Download and execute the *EUM_Agent.exe* file. The installshield wizard will open up.
2. Read the license agreement and click the **Yes** button.
3. Specify the details of your Applications Manager installation such as host, port, username and password. Click Next to proceed.
4. Provide the location where the EUM agent 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 End User Monitoring Agent**. Click **Next**.
6. If you want to install EUM as a service, select the '**Install End User Monitoring Agent as Service**' option and click Next. Please note that you need to have administrative privileges to install the EUM agent as a service.
7. The current settings will be displayed in the next screen. If you need to make any changes, click Back, or else click Next to continue with the installation. Once you click Next, the setup will start copying the jar files necessary for the EUM agent.
8. You have an option to fill up a registration form for technical support.

9. In the final step of the installation wizard, there are options available to *View the Readme file* and to *Launch the End User Monitoring Agent Now*. Select these options if required. Click **Finish** to complete the installation process.

Linux

Follow the steps given below to install the EUM agent in Linux systems.

1. Download the *EUM_Agent.bin* file for Linux.
2. Execute the downloaded file. The Installation Wizard is displayed. Click **Next** to continue. Read the license agreement and click the **Next** button.
3. Provide the **location** where the EUM agent should be installed in your machine. Click **Next**.
4. Current Settings will be displayed in the next screen. If you need to make changes, click **Back**, else click **Next** to continue the installation.
5. Click **Finish** to complete the installation process.
6. You have an option to fill up a **registration form** for Technical support.
7. Finally, select if you want to view the **ReadMe** file or click **Finish** to launch the EUM agent immediately.

Note:

1) You can also install the EUM agent via **command line**. Just type in the following command in the command prompt:

```
./EUM_Agent.bin -console
```

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

2) The Real Browser Monitor (RBM) will not work if you install the EUM agent in Linux systems. This is because the RBM requires Internet Explorer browser for playback.

Uninstalling EUM Agent

In Windows:

1. If the EUM agent is running, you should stop the agent before uninstalling it. You can stop the agent using any of these options:
 1. Use the *Start menu->All Programs->ManageEngine EndUser Monitoring Agent->Stop Server* option.
 2. From the command prompt, execute the *StopServer.bat* file present under the <ManageEngine/EUMAgent> folder.

2. Use the *Start menu->All Programs->ManageEngine EndUser Monitoring Agent->Uninstall* option. The installshield wizard will be displayed. Follow the instructions shown on screen to uninstall the agent.
3. Remove the agent completely using the *Control Panel->Add/Remove Programs* option.

In Linux:

1. From the command line, go to the Applications Manager Home directory and execute the below commands:


```
sh shutdownApplicationsManager.sh  
sh shutdownApplicationsManager.sh -force
```
2. Exit out of the command prompt and close all the files and folders opened in the Applications Manager Home directory.
3. Execute the command `./uninstaller.bin` from the `<AppManager/_uninst>` directory.

End User Monitoring Agent Settings

When you start the End User Monitoring agent, the EUM web client will be automatically launched. The web client can be accessed at `http://localhost:<PORT>` url where localhost is the system where the EUM agent is installed and PORT is the port number where the EUM agent is running.

You can modify the EUM agent settings from the EUM agent web client by clicking the *Edit* button and updating the settings. These changes will take effect only when you restart the agent.

EUM Dashboard

The performance metrics of all the end user monitoring (EUM) monitors configured in Applications Manager will be displayed in the **End User Monitoring Overview** dashboard under the 'EUM' tab. This dashboard provides you an overview of the performance of your monitors tracked using EUM agents along with their health status from different locations. The metrics shown include the total number of EUM monitors and their current status (Clear, Critical or Warning), the category to which the monitor belongs to, and their health status from the locations configured.

A green dot indicates health status is 'clear' from that specific location, a red dot indicates 'critical' status while an orange dot indicates 'warning' health status. Click the dot icon to drill down into the monitor performance from that specific location. Click the reports icon in the EUM dashboard to view the 'At a Glance' report for the monitor. The 'At a Glance' report includes charts for availability, response time and outage report of the monitor from different locations.

You can also view performance details based on the monitor type. For example, to view information about DNS monitors, click the DNS Monitor icon.

EUM Agent Details

Click the 'Locations' link present in the right top corner of the 'End User Monitoring Overview' dashboard to view details about the EUM agents being used to collect performance data. This screen shows the following agent configuration details:

Parameter	Description
Name	The name of the EUM agent
IP Address	The IP address of the EUM agent
Port	The port at which the agent is running
Status	Current status of the agent (whether the agent is up or down)
Poll Interval	The time interval in which the EUM agent contacts the Applications Manager server
Agent Version	The version of the EUM agent currently in use
Last Updated at	The time at which agent collected information from the Applications Manager server

APM Insight - An Overview

APM Insight (previously J2EE Transaction Monitoring) gives you visibility into the way your applications behave for your end users. You get comprehensive end-to-end transaction awareness across your entire infrastructure, enabling you to isolate performance issues and resolve them quickly. Drill-down to the root cause of problems quickly and perform first-level troubleshooting.

With so many different metrics being produced by the wide range of business applications, how can one normalize performance and assemble information into something meaningful to the end users? APM Insight offers visual representations of performance metrics of all components starting from URLs to SQL queries, Apdex scores to measure user satisfaction and transaction tracing.

You can view the trace history of transactions to help identify and resolve performance degradation no matter where they originate. Further, to identify bottlenecks in performance, a trail of the Java method invocations can be viewed to identify the offending code.

Browse through the following topics to understand the working of APM Insight:

- [How Does APM Insight Work?](#)
- [Installing APM Insight Agent](#)
- [APM Insight Configuration Options](#)
- [APM Insight Dashboard](#)
 - [Web Transaction, Database Operations and Transaction Traces](#)
 - [Apdex Score](#)

How does APM Insight work?

APM Insight includes a remote monitoring agent to be deployed in your Application Server. This agent performs the tasks of data collection; acquisition and transmission.

To configure APM Insight you must first download the APM Insight agent and deploy it in your Application Server. Once the agent is deployed, the agent residing in the Application Server uses byte code instrumentation to collect application performance metrics and sends it to the central Applications Manager server at fixed intervals.

APM Insight gives you the following metrics for the applications that it is set to monitor:

- APDEX Scores
- Response Time
- Throughput

Based on the metrics received from the agent, the APM Insight server measures the performance of the application and generates performance charts. This information is assembled and presented in detail in the APM Insight dashboard.

How to install APM Insight?

- Download and install
- Configure agent

When the Application Server starts up, APM Insight Monitor will be added automatically in the Applications Manager.

Installing the APM Insight Agent

APM Insight relies on the agent-based instrumentation technology for data acquisition and transmission.

- Web Components supported: JSP, Servlets, EJB
- Web Frameworks supported: Struts
- ORM Frameworks supported: Hibernate, Spring, iBATIS

This section covers the following topics on installing the APM Insight Java Agent:

- Deploying APM Insight Java Agent in Apache Tomcat
 - Installing within a Service in a Windows Platform.
 - Using catalina.bat to start the Server in Windows Platform.
 - Using catalina.sh to start the Server in linux Platform.
- Deploying APM Insight Java Agent in WebSphere
- Deploying APM Insight Java Agent in JBoss
- Deploying APM Insight Java Agent in WebLogic
- Deploying APM Insight Java Agent in other servers

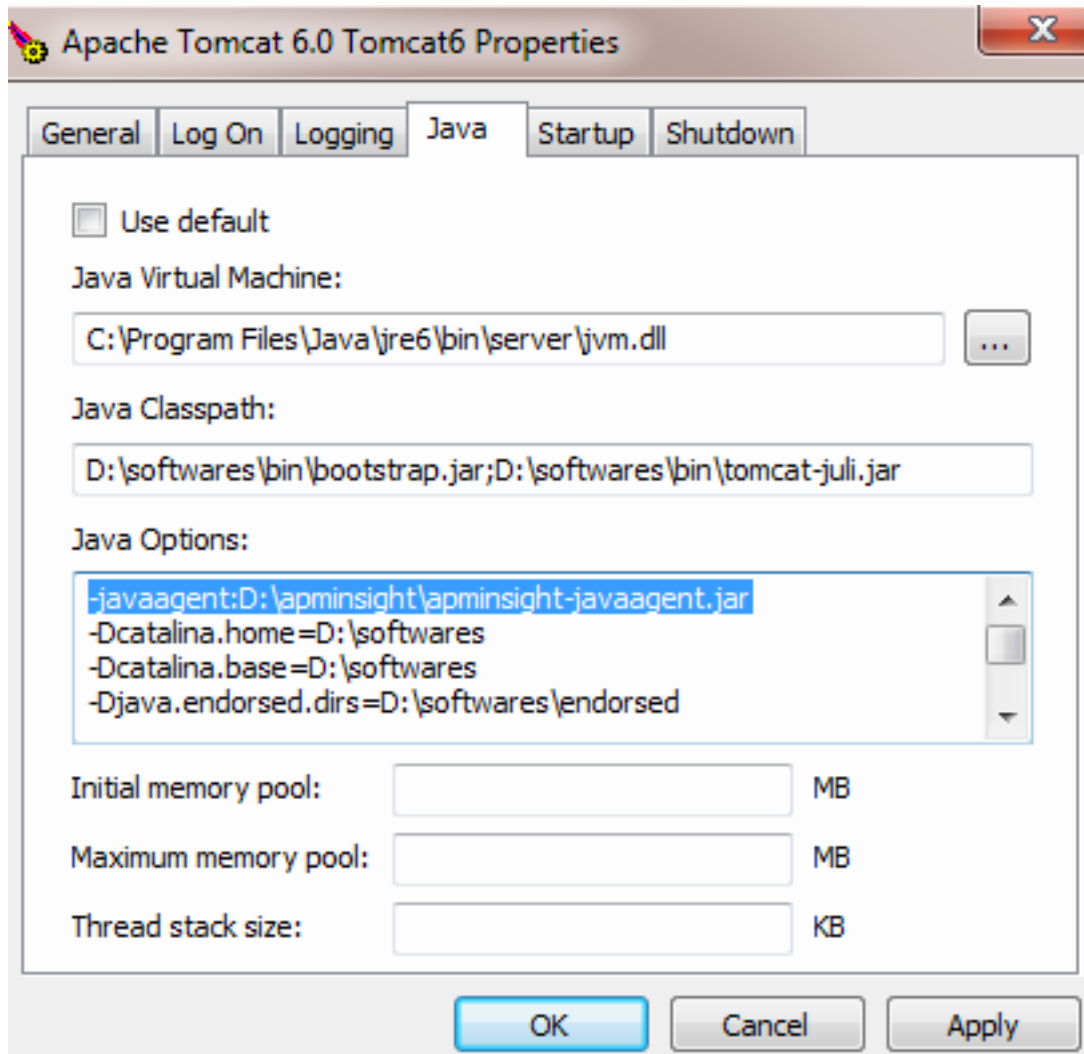
Installing APM Insight Java Agent in Apache Tomcat:

APM Insight can be installed in Apache Tomcat server using the following methods:

Installing within a Service in a Windows Platform:

You can deploy APM Insight within Apache Tomcat which is installed as a service in a Windows platform.

- Download apminsight-javaagent.zip
- Extract the zip to find apminsight-javaagent.jar and its configuration file apminsight.conf
- Move the two files to a new directory, say apminsight created inside tomcat_home
- tomcat_home is the location where the Apache Tomcat Server is installed eg:
c:/softwares/apache-tomcat/apminsight
- Navigate to Configure Tomcat --> JAVA tab and add JavaAgent entry -
javaagent:D:\apminsight\apminsight-javaagent.jar in Java Options box as shown below.
- The Apache Tomcat Properties Window can also be accessed by right clicking Tomcat Icon in system tray and selecting the Configure option.



- After adding the Java Agent entry, click on Apply. Then click OK.
- Navigate to <tomcat_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key application.name eg: application.name=JpetStore.
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid Applications Manager host address & Port in apminsight.conf for the keys apm.host & apm.port respectively. eg: apm.host=myapmmachine.mydomain.com. apm.port=9090

More configurable options of APM Insight Java Agent can be found here

Using catalina.bat to start the Server in Windows Platform:

You can install APM Insight using catalina.bat batch file to start the server in Windows Platform.

- Download apminsight-javaagent.zip
- Extract the zip to find apminsight-javaagent.jar and it's configuration file apminsight.conf

- Move the two files to a new directory say, apminsight created inside tomcat_home
- tomcat_home is the location where the Apache Tomcat Server is installed eg:
c:/softwares/apache-tomcat/apminsight
- Open catalina.bat in <tomcat_home>/bin folder using a text editor
- Add the following entry at the top of the file- SET JAVA_OPTS=%JAVA_OPTS% -
javaagent:<path-to- apminsight>/apminsight-javaagent.jar eg: SET
JAVA_OPTS=%JAVA_OPTS% -javaagent:c:/softwares/apache-
tomcat/apminsight/apminsight-javaagent.jar
- Navigate to <tomcat_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key
application.name eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid
Applications Manger host address & port in apminsight.conf for the keys apm.host & apm.port
respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090

More configurable options of APM Insight Java Agent can be found here

Using catalina.sh to start the Server in Linux Platform:

You can also install APM Insight using catalina.bat shell script file to start the server in Linux Platform.

- Download apminsight-javaagent.zip
- Extract the zip to find apminsight-javaagent.jar and it's configuration file apminsight.conf
- Move the two files to a new directory say, apminsight created inside tomcat_home
- tomcat_home is the location where the Apache Tomcat Server is installed eg:
/home/local/softwares/apache-tomcat/apminsight
- Open catalina.sh in <tomcat_home>/bin folder using a text editor
- Add the following entry in top of the file.
- SET JAVA_OPTS=%JAVA_OPTS% -javaagent:<path-to- apminsight>/apminsight-
javaagent.jar eg: SET JAVA_OPTS=%JAVA_OPTS% -
javaagent:/home/local/softwares/apache-tomcat/apminsight/apminsight- javaagent.jar
- Navigate to <tomcat_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key
application.name. eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid
Applications Manger host address & Port in apminsight.conf for the keys apm.host & apm.port
respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090

More configurable options of APM Insight Java Agent can be found here

Deploying APM Insight Java Agent in WebSphere

APM Insight Java Agent can be deployed in Websphere through Admin Console as follows:

- Download apminsight-javaagent.zip
- Alternatively you can also find apminsight.zip in
<applications_manager_home_directory>/working/resources
- Extract the zip to find apminsight-javaagent.jar and it's configuration file apminsight.conf
- Move the two files to a new directory say, apminsight created inside websphere_home
- websphere_home is the location where the WebSphere Application Server is installed eg:
c:/softwares/IBM/WebSphere/AppServer/apminsight
- Login as admin in console
- Expand Servers tree option in the left and click on Application Servers
- Select the Server in which you are going to install the java agent
- Under Server Infrastructure, expand JAVA and Process Management and click on Process Definition.

The screenshot shows the Admin Console interface. On the left, the 'Servers' tree is expanded, and 'Application servers' is selected. The main panel displays the 'Application servers' configuration page. It includes a description: 'An application server is a server which provides services required to run...'. Below this, there is a 'Preferences' section with a table of application servers.

Select	Name	Ncde
<input type="checkbox"/>	server1	app-xp4Node01

Total 1

- Under Additional Properties, Click on Java Virtual Machine
- In Generic JVM arguments box add the following line,
-javaagent:<path-to-websphere_home>/apminsight-javaagent.jar
eg: -javaagent:c:/softwares/IBM/WebSphere/AppServer/apminsight/apminsight-javaagent.jar
Note: The agent path is actually the Application Server's machine path.
- If more statements are found in the box, use blank space as separator.
- Click on Apply and then Save.

Initial Heap Size

Maximum Heap Size

☐ Run HProf

HProf Arguments

☐ Debug Mode

Debug arguments

Generic JVM arguments

Executable JAR file name

☐ Disable JIT

Operating system name

- Navigate to <websphere_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key application.name eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid Applications Manager host address & Port in apminsight.conf for the keys apm.host & apm.port respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090

More configurable options of APM Insight Java Agent can be found here

Deploying APM Insight Java Agent in JBoss

- Download apminsight-javaagent.zip
- Extract the zip file to find apminsight-javaagent.jar and it's configuration file apminsight.conf
- Move the two files to a new directory say, apminsight created inside jboss_home
- jboss_home is the location where the JBoss Application Server is installed eg:
c:/softwares/jboss/apminsight
- Open the run.bat in <jboss_home>/bin folder using a text editor
- Add the following entry in top of the file,
- SET JAVA_OPTS=%JAVA_OPTS% -javaagent:<path-to-jboss_home>/apminsight-javaagent.jar

- Navigate to <jboss_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key application.name eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid Applications Manager host address & Port in apminsight.conf for the keys apm.host & apm.port respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090.

More configurable options of APM Insight Java Agent can be found here

Deploying APM Insight Java Agent in WebLogic

- Download apminsight-javaagent.zip
- Extract the zip to find apminsight-javaagent.jar and its configuration file apminsight.conf
- Move the two files to a new directory say, apminsight created inside weblogic_home ; weblogic_home being the location where the WebLogic Application Server is installed eg: c:/softwares/bea/weblogic/server/apminsight
- Open the startWLS.bat in <weblogic-home>/bin folder
- Add the following entry in top of the file,
SET JAVA_OPTIONS=%JAVA_OPTIONS% -javaagent:<path-to-weblogic_home>/apminsight/apminsight-javaagent.jar
- Navigate to <weblogic_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key application.name eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid Applications Manager host address & Port in apminsight.conf for the keys apm.host & apm.port respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090

More configurable options of APM Insight Java Agent can be found here.

Deploying APM Insight Java Agent in Other Servers

- Download apminsight-javaagent.zip
- Extract the zip to find apminsight-javaagent.jar and its configuration file apminsight.conf
- Move the two files to a new directory say, apminsight created inside Application_Server_Home ; Application_Server_Home being the location where your Application Server is installed.
- Find your Application Server startup script and open it in a Text Editor.
- Add the following entry in top of the file,
SET JAVA_OPTS=%JAVA_OPTS% -javaagent:<path-to-application_server_home>/apminsight/apminsight-javaagent.jar

- Navigate to <application_server_home>/apminsight directory to find apminsight.conf
- Open the file with a text editor and enter a suitable Application Name for the key application.name eg: application.name=JpetStore
- Make APM Insight Java Agent to communicate with Applications Manager by entering valid Applications Manager host address & Port in apminsight.conf for the keys apm.host & apm.port respectively. eg: apm.host=myapmmachine .mydomain.com apm.port=9090

More configurable options of APM Insight Java Agent can be found [here](#).

APM Insight Agent Configuration Options

APM Insight Agent works based on the values configured in apminsight.conf file. Make sure that this file is present in the folder where you have deployed the apminsight-javaagent.jar.

The following table explains all the configurations:

Configuration	Description	Default Value
* application.name	Specify the desired Application's Name to show in Applications Manager. If there are multiple instances of your application and you would like to group them, then specify the same application name in all installed APM Insight Agent Configuration files. Example: myonlineshopping.com	
* apm.host	Host Name where the Applications Manager is running. If an invalid/ unreachable host names is entered, the agent throws a 'Connection Refused' Exception and the agent will shut itself down. However the Application Server will be started. It accepts either the host name or an Ipv4 address Example: mymachine.mydomain.com	
apm.protocol.https	Specify true if the data to the Applications Manager should be sent through HTTPS Protocol. If false, data will be sent through HTTP Protocol	Default value: false
* apm.port	Specify the HTTP Port of the Applications Manager. If apm.protocol.https is true, specify the HTTPS Port. If the service is not running in the specified port, the agent throws a 'Connection	

Configuration	Description	Default Value
	<p>Refused' Exception and the agent will shut itself down. However, the Application Server will be started.</p> <p>Example: 9090</p>	
behind.proxy	<p>Specify whether the Agent installed Application Server is under a proxy network. If set True, Proxy credential information should be given in order to send the metric data from the agent to Applications Manager. If behind.proxy is set to true, specify values for the following keys:</p> <p>proxy.server.host: Host name of the proxy server</p> <p>proxy.server.port: Proxy server's port</p> <p>proxy.auth.username: User name of the proxy server</p> <p>proxy.auth.password: password for the proxy server</p>	<p>Default value: false</p>
* agent.server.port	<p>Specify the HTTP listening port of the Application Server.</p> <p>It will be useful to distinguish Instances when more than one Application Server runs in same host.</p> <p>Example: 8080</p>	
apdex.threshold	<p>Application Performance Index (simply called Apdex) is measurement of an Application's Performance ranging from 0 to 1. Detailed information about Apdex can be found at www.apdex.org</p> <p>If any transaction response time scores values below the apdex.threshold value, the transaction is labeled as Satisfied.</p> <p>If any transaction response time scores above four times the apdex.threshold, the transaction is labeled as Frustrated.</p>	<p>Default value: 0.5 (Second)</p>

Configuration	Description	Default Value
	If it is exactly equal to apdex.threshold or in between satisfied and frustrated threshold value it is labeled as Tolerating.	
sql.capture.enabled	<p>Enabling this option will listen to all SQL Queries which gets executed.</p> <p>If this option is disabled, no Database Metrics will be collected.</p>	Default value: true
transaction.trace.enabled	<p>Enabling this option will construct Trace for Slow Transactions.</p> <p>You can view the traces collected in Applications Manger APM Insight Page by selecting Traces tab.</p>	Default value: true
transaction.trace.threshold	<p>Trace of any transaction whose response time scoring above the specified threshold value will be collected, provided if transaction.trace.enabled is set to true.</p> <p>The trace can be used to analyze, troubleshoot the transaction working.</p>	Default value: 1 (Second)
transaction.trace.sql.parametrize	<p>Enabling this option will parametrize all SQL Queries in Slow Transaction Traces. (if sql.capture.enabled set to true & transaction.trace.enabled set to true)</p> <p>Disabling this option will give you the real query (with parameters).</p> <p>It is recommended to enable this option if there are queries getting executed using confidential parameters like credit card number, passwords, etc.</p>	Default value: true
transaction.trace.sql.stacktrace.threshold	<p>Enabling this option will collect the stacktrace whenever any sql query executed above this threshold time value.</p>	Default value: 3 (Second)

Configuration	Description	Default Value
include.packages	<p>APM Insight does not instrument all the classes loaded. APM Insight itself has a predefined list and only those classes will be instrumented.</p> <p>If you need to instrument any of the other classes, you can achieve this by specifying the package name of the class.</p> <p>Use Comma to separate multiple entries</p> <p>For eg.,</p> <p>include.packages=com/test/customimpl/. * will include all the packages & classes that start with com.test.customimpl</p>	
transaction.tracking.request.interval	<p>A kind of sampling. If said 20, apminsight will only track request after every 20 requests of same kind. i.e it will track 1st, 21st, 41st.. request of its kind.</p> <p>The request count maintained will be reset after every one minute.</p>	Default value: 1 (request)
apminsight.log.dir	<p>Directory path where the APM Insight log should be stored.</p> <p>Use backslash(\) as path separator</p> <p>example: D:\Tomcat6.0\apminsight</p> <p>Defaults to the directory where APM Insight agent jar is installed if commented or mentioned incorrectly or unable to create the configured directory.</p>	
apminsight.log.level	<p>The log level at which the APM Insight agent should record information.</p> <p>Supported levels are SEVERE,WARNING, INFO and FINE.</p>	Default value: INFO (level)

APM Insight will use its default factory value if any invalid value specified for an option.
Other than options listed below, all the other options can be changed at run time.

- application.name
- apm.host
- agent.server.port
- apminsight.log.dir
- apminsight.log.level

Note:

Options marked with a * are mandatory. If any of the mandatory files are not provided, the Agent cannot be initialized / started. However the Application Server (where the Agent is deployed) will start normally.

For more detailed information about APDEX threshold go to : www.apdex.org

APM Insight Dashboard

The performance of complex, distributed applications can be efficiently monitored only when data is presented in a simple and impactful manner. APM Insight's customized dashboards help you understand your applications at a single glance!

The performance metrics of the applications being monitored in APM Insight is displayed under the 'APM Insight' tab. These metrics include mainly:

- Application Performance Index (APDEX)
- Response Time, and
- Throughput

The 'Show By' option in the dashboard on the APM Insight page gives you two different views to summarize these metrics:

- Application Level view
- Instance Level view

The Application Level view displays combined results of all the instances running in a particular application.

The drop down list in the top right-hand corner of the page gives you the option to view the details from the Last 1 Hour to the Last 1 Day.

To view detailed performance metrics, click the corresponding listed Instance. The metrics are categorized into three different tabs for better understanding:

- Web Transaction & Apdex scores.
- Database Operations
- Transaction Traces

To view Reports on the metrics for the APM Insight monitor click on Reports from the main tab and then select Trend Analysis Report from the list at the left.

The following report types are displayed:

- At a glance Report
- Downtime History
- Summary Report of Monitor

Web Transaction

The Web Transaction page will give you details pertaining to the action that consumes longer time, frequently accessed actions, tier-wise breakdown of transaction response time (Example: JVM, Database, and much more) from the application level down to the individual transaction level.

The transactions can be sorted out on the basis of Most Time Consuming , Throughput, Lowest Apdex and Slowest Average Response.

Transaction Trace

The Transaction tracing feature will provide you with insight into individual transactions. Transaction Traces are snapshots of transactions to help you identify performance bottlenecks by drilling down the transactions to pinpoint the cause of trouble.

Based on your configuration in apminsight.conf, the SQL Statements executed within the transaction and its stack trace are collected and displayed in tree view.

In the trace page transactions are assembled with various parameters like:

- Transaction Start Time
- Transaction Response Time
- Transaction Average Response Time

Database operations

With APM Insight you can get detailed performance metrics to identify the slow database calls, database usage and overall performance of the database furnished with detailed graphical and tabular representations.

By clicking on individual database operation, you get a list of web transactions that were performed by this particular table, thereby helping you to narrow down and isolate the root cause of performance slowdown.

In the **Database** page you can view all the database operations and represent them as charts based on:

- Overall Database Response Time and Throughput
- Database Response Time by Operation
- Database Throughput by Operation

Database operations can be sorted on the basis of:

- Slowest average response time.
- Throughput
- Most time-consuming

Note:

You can switch between the graphical or tabular representation of the webtransaction and database operations page using the Graph View and Table View buttons at the right-hand corner of the page.

Apdex Score

Apdex (Application Performance Index) is an open standard to measure the user satisfaction regarding a web application. It is a metric that provides a single score ranging between 0-1 (0 = no users satisfied, 1 = all users satisfied), giving business application owners an insight into the measure of their customer happiness and satisfaction levels.

Easy to calculate and interpret, the data collected over a period of time are converted into a simple index based on the application responsiveness. Application responsiveness is categorized into three zone based on the Apdex score:

1. **Satisfied:** This represents the time value (T seconds) below which users are not impeded by application response time. Depicts the user is fully productive.
2. **Tolerating:** This represents response time greater than T (precisely, T to 4T), where the user notices performance lagging but continues the process, which depicts the response is tolerated by the user.
3. **Frustrated:** This represents response time F, greater than 4T which is unacceptable, and users may abandon the process, which depicts the user is frustrated.

The value T can be defined by the application owners

The Apdex Score is calculated using the following formula:

$$\text{Apdex} = \frac{\text{Satisfied Count} + \frac{\text{Tolerating Count}}{2}}{\text{Total Samples}}$$

The score of 1 show all the users are satisfied with the application performance, whereas a score of 0 show no users are satisfied. Score of 0.5 shows all the users are tolerating the application performance. As the application responsiveness vary, the score ranges from 0-1.

Apdex Score, as a whole, is critical to measure the service levels and customer satisfaction which in turn measures the business growth. Moreover, these values are easy to decipher; unlike the traditional values of average response time and throughput, that does not accurately interpret a particular transaction that is performing slow and affect user satisfaction.

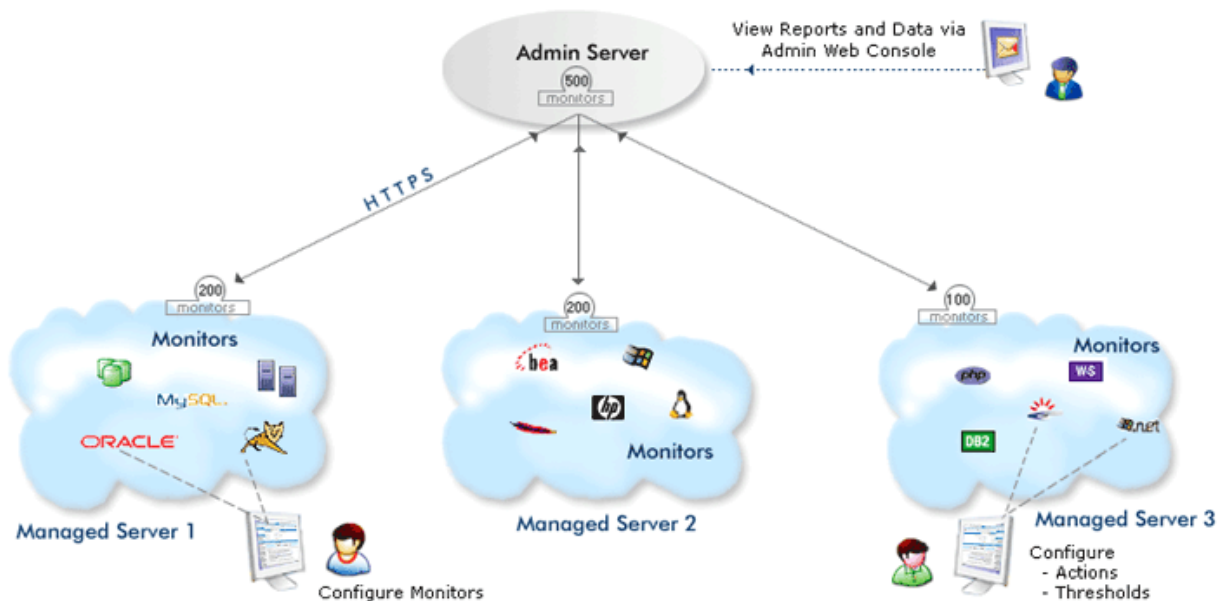
Enterprise Edition

ManageEngine Applications Manager Enterprise Edition allows you to monitor more number of servers and applications in a **distributed setup**. You can configure independent Applications Manager installations to monitor resources and then collectively view the data from all these independent Applications Manager installations ("**Managed Server**") from a single installation ("**Admin Server**").

Installation & Setup

- During installation, you will be provided with options of selecting the type of installation as *Free/Professional/Enterprise* Edition
- On choosing Enterprise Edition, you would be asked to choose whether you want the installation to be that of Admin Server or Managed Server
- In Enterprise Setup, you must first configure the Admin Server and then configure the Managed Server
- **Admin Server:** Enter the WebServer and SSL port and continue with installation.
- **Managed Server:** Enter the Admin server Host Name, SSL Port (8443 by default) and WebServer port. Select the Proxy Settings needed to contact the Admin Server if needed (This is a separate step in Linux but not so in Windows Installation)

Applications Manager Enterprise Edition - Architecture



Enterprise Edition Overview

As a first step, Admin Server has to be started. When a Managed Server starts, it contacts the Admin Server for registering itself (based on the Admin Host/ SSL Port provided during installation). The Admin Server assigns a unique ID to this Managed Server called the "Server ID". Each managed

Server is identified by its Server ID. Every 5 minutes, the Admin Server contacts the Managed Servers that are registered to it and fetches the required data from each of the Managed Servers. You can view all the data from the Managed Servers in the Admin Server console itself.

Converting the Professional Edition to Enterprise Edition

If you are using Applications Manager as a standalone server (Professional) and want to convert it into a distributed setup (Enterprise Edition) without losing the Configuration Information, you will have to do the following steps :

- Do a fresh installation of **Admin** server of Applications Manager and start the same.
- Now, in the existing standalone Application Manager 's, Click on link **Convert standalone server into Managed Server** under the 'Admin tab - Global Settings". (You can convert only one standalone server to Managed server. You can add more Managed Servers through fresh installations.)
- You will have a popup requesting details of the Admin Server Host and Admin Server SSL port. Provide the details to complete the conversion from Standalone server to Managed Server.
- You can verify from the Support Tab if the type of Server is Managed Server.

Note: It is possible to convert a Standalone installation to a Managed Server only if there are no other Managed Servers already added to the Admin server i.e., only if you are just installing a new Admin Server. If you already have a Enterprise Setup (Admin Server/Managed Server), you cannot convert a Standalone Server to be a part of the setup. It is not possible to change from Admin server type to a Standalone setup or vice versa without reinstalling the product.

Warnings: It is not possible to revert from Managed server back to Standalone setup although it will still be functioning without any problems

Know more about the functioning of Admin Servers and Managed Servers.

Note: Visit Enterprise Edition FAQ for details on when to, how to set up Enterprise Edition

Enterprise Edition - Admin Server

Enterprise Edition Admin Server is the master server through which you will be able to view consolidated data of all the Managed Servers.

Installation

During installation, you need to select the Edition option as 'Enterprise Edition'. Next select the installation type as 'Admin Server'. Then, you need to enter the *HostName*, *WebServer port*, *SSL port* of the *Admin Server*. Kindly carry on with the rest of the installation process.

Managed Server Configuration

The Managed Server automatically gets registered with the Admin Server when it starts up. In case you want to edit the configuration, go to Admin tab. Click on Managed Servers link. This will take you to the Managed Server page from where you can configure the Managed Servers. Alternatively, this can be done by clicking on the Managed Servers link just below the main tabs.

Steps to Add a Managed Server

- Click on the **Add New** link, it opens up the **Add New Managed Server** form
- Enter the **Host Name** of the Managed Server
- Enter the **Web Server Port** number, the port at which the web client is to be connected
- Enter the **SSL port** number, the port at which secure communication is to be made between the Admin and Managed Server.
- Enter the **Server ID**, the ID present under *Installation Information* table under *Support Tab* of the Managed Server
- Enter the **Admin Password** for the Managed Server. (**Note:** This password should be same as that of Admin role password of that managed server. If user changes that password in the Managed server, then the user has to manually update the same in admin server)
- Click on **Add Managed Server** and the Managed Server gets added. It is displayed under Managed Servers link along with the details of the number of monitors, status, load factor, etc.,

Note: In order to find if a particular Applications Manager installation is heavily loaded you can use the **Load Factor**, which is provided in the 'Support' tab under the 'Applications Manager Installation Information' category. The **load factor** follows the format x.y, where 'x' represents load on Applications Manager Server, while 'y' represents the load on the Database used by Applications Manager. A value of zero represents least loaded, while a value of nine represents most loaded. Hence Load Factor can take values from 0.0 to 9.9 (heavily loaded). The Load Factor of each of the Managed Servers is also displayed in the Admin server under the "Managed Servers" option and you can use the same to distribute load evenly among the Managed Servers.

Creating Monitor Groups in Admin Server

Various monitors in Managed Servers can be grouped and a consolidated view can be obtained in Admin Server. For eg., consider a set up that has three Managed Servers and one Admin Server. Each Managed Server has 200 monitors which includes 10 windows servers. If you want to monitor the windows servers in all the three managed servers as a group, then you can create a new Monitor Group in the admin server.

You can create Monitor Groups by following the steps in Create Monitor Group help document. Once you have created the Monitor Group, the next step would be to associate the required monitors from Managed Servers to the Monitor Group in the Admin Server. After the setup is done, you can configure the alarms for the Monitor Group. Currently, only EMail and SMS alarm actions are supported.

Actions

Fetch Data: There is an option to fetch the data from the managed servers at the given instant, instead of waiting for the poll to happen.

Edit: You can edit the managed server details using this option.

Enable/Disable: You can enable/disable data collection in the Managed Server. Note that when you disable, data collection will still take place, you only stop syncing with the managed server.

Admin Email Settings: An EMail can be configured to be sent once a Managed Server goes down and also once every 24 hrs till the Managed Server is up again. The EMail setting is available in the Admin EMail Settings" option under the "Admin" tab. The option to enable/disable this EMail, is available in the "Edit" option of the respective Managed Server.

Proxy Managed Server request through Admin Server: When you login to the Admin console, Graphs and images displayed for a monitor are retrieved directly from the corresponding Managed Server itself and are displayed in the Admin console. These graphs/images cannot be retrieved, if the Admin Server is accessible from a particular machine/over the Internet and the Managed Server is not accessible.

In this case, select the "*Proxy Managed Server request through Admin Server*" request option. This will result in the images/graphs being fetched to the Admin Server from the Managed Server first and then the image from the Admin Server is viewable in the Web Browser.

E.g., Admin Server is running as part of IDC and accessible via the Internet (From a machine say "ClientMachine") but the Managed Servers are not accessible (from "ClientMachine") this option should be enabled.

User Administration: In the Enterprise setup, the User Administration module functions independently in the Admin Server and Managed Server. Hence, a user-based view assigned in the Managed Server will not reflect in the Admin Server and vice-versa. Since, you will be viewing the data collectively from the Admin Server, you need to assign owners to the various Monitor Groups of the Managed Server in the Admin Server. Of course, if it is assigned in the Managed Server it will function independently. Also, in the Manager Console (SLA Management console), you can assign SLAs and associate actions to be invoked for SLA violation to the Monitor Groups in the Admin Server.

Managed Server Access

Click on the **Jump To** link in the Admin Server just above the toolbar, which brings down a list of the Managed Servers. Clicking on any of the Managed Server names in the list will take you to the web console of the respective Managed Server in a separate browser Window.

Note: ENTERPRISEADMIN role is used for logging into the Managed Server from Admin Server for data synchronising. The username for this role is systemadmin_enterprise and the password is the regular ADMIN role password. This role is not exposed in the UI, it will be used internally.

Important: Visit Enterprise Edition FAQ for details on when and how to set up the Enterprise Edition.

Enterprise Edition - Managed Server

Enterprise Edition allows you to configure independent Applications Manager installations to monitor various resources and then collectively view the data from all these independent Applications Manager installations known as **Managed Servers**, from a single master server known as **Admin Server**.

During installation, you need to select 'Enterprise Edition'. Next select the installation type as 'Managed Server'. Consequently, you need to enter the *HostName*, *SSL & webserver port* of the *Admin Server*, to which the Managed Server is going to be connected. Managed Server's function is similar to that of a standalone Applications Manager, with the user configuring the various monitors, thresholds and alarms. HTTPS mode of communication is used for the communication with the Admin Server.

Using the *Jump To* link in the Admin Server (just above the toolbar) you can view the Managed Server web console.

To **change a Professional Edition to Managed Server**, go to *Global Settings*, select '**Convert standalone server into Managed Server**'.

Note: This option is available only if you have installed the full build and not for upgrades through PPM.

Note: Visit Enterprise Edition FAQ for details on when to, how to set up Enterprise Edition.

Enterprise Edition - Failover Support

There are two methods of implementing failover support in ManageEngine Applications Manager:

1. Single Database - Dual AppServer Architecture
2. Dual Database - Dual AppServer Architecture

Single Database - Dual AppServer Architecture

This setup involves a primary Applications Manager, a secondary Applications Manager and a common database. The primary and secondary Applications Manager refer to the common database only. While the primary Applications Manager talks with the database, the secondary Applications Manager simply listens to the database. If the primary server goes down, the secondary server takes over. Afterwards, the initial primary server is restarted and it starts functioning as a secondary server.

Failover Setup Details

Let us assume we are going to set up three nodes - node1, node2 and node3.

Applications Manager: node1, node2

MySQL Database: node3

Configuring the MySQL Server in node 3:

- Install **MySQL database Server version 4.0.13** in node3 and start the MySQL Server.
- Otherwise, take the MySQL bundled in Applications Manager itself. For this,
 - Go to *C:\Program Files\ManageEngine\AppManager10\working* directory.
Take the zip of the contents in mysql folder.
`zip -r mysql.zip mysql*`
 - Go to *C:\Program Files\ManageEngine\AppManager10\working\bin* folder and add the *startMySQL.bat* and *stopMySQL.bat* in the mysql.zip.
`zip startMySQL.bat stopMySQL.bat mysql.zip`
 - Take this zip and extract the contents in a folder in node3.
 - Execute the *startMySQL.bat* file

This will start the MySQL Database Server.

By default, this MySQL is configured in such a way that it accepts connections for the machine in which the Applications Manager is installed. Hence, you need to add entries for the hosts node1 and node2 to access this database.

Please refer the below link for configuring permissions.

http://manageengine.com/products/applications_manager/troubleshoot.html#m20

For **stopping** the MySQL database, you can use the *stopMySQL.bat*.

[Open this file and change the line "*set MYSQL_HOME=..\mysql*" to "*set MYSQL_HOME=.\mysql*"]

Installing Applications Manager in node1 and node 2

After installing Applications Manager in node1 and node2, do the following configurations

For Windows:

By default AppManager10 - C:\Program Files\ManageEngine\AppManager10\

- AppManager10\conf\AMServer.properties - Change *am.mysql.port* to the MySQL port number (eg: *am.mysql.port=3306*)
- AppManager10\conf\AMServer.properties - Change *am.mysqlport.check* to false (eg: *am.mysqlport.check=false*)
- AppManager10\working\conf\database_params.conf - Change *jdbc:mysql://localhost:13326/AMDB* to *jdbc:mysql://node3:mysqlport/databasename* (eg: *jdbc:mysql://localhost:3306/MADB*)
- AppManager10\working\conf\database_params.conf - Change username & password fields as required
- AppManager10\working\bin\startMySQL.bat - Comment the line starting with *mysqld-nt* (eg: *rem mysqld-nt ..*)
- AppManager10\working\bin\stopMySQL.bat - Comment the line starting with *mysqladmin* (eg: *rem mysqladmin ..*)

For Linux:

By default AppManager10 - /opt/ManageEngine/AppManager10

- AppManager10/conf/AMServer.properties - Change *am.mysql.port* to the MySQL port number (eg: *am.mysql.port=3306*)
- AppManager10/conf/AMServer.properties - Change *am.mysqlport.check* to false (eg: *am.mysqlport.check=false*)
- AppManager10/working/conf/database_params.conf - Change *jdbc:mysql://localhost:13326/AMDB* to *jdbc:mysql://node:mysqlport/databasename* (eg: *jdbc:mysql://localhost:3306/MADB*)
- AppManager10/working/conf/database_params.conf - Change username & password fields as required
- AppManager10/startApplicationsManager.sh - Comment the 3 lines *if [\$? != 51]; then , . \$NMS_HOME/bin/stopMySQL.sh* and *fi* using *#* in that file.

Sample Files:

AMServer.properties

am.mysql.port=3306

am.mysqlport.check=false

database_params.conf

url jdbc:mysql://**appmanager:3306/APPMANAGERDB** AppModule TopoDB-MapDB-EventDB-AlertDB-PollDB-PolicyDB-USERSTORAGEDB-ApplnDB

username **admin** AppModule TopoDB-MapDB-EventDB-AlertDB-PollDB-PolicyDB-USERSTORAGEDB-ApplnDB

password **appmanager** AppModule TopoDB-MapDB-EventDB-AlertDB-PollDB-PolicyDB-USERSTORAGEDB-ApplnDB

Note: If your MySQL does not require a password to connect, the password line in `<database_params.conf>` should be commented as shown in the above example using the #. Otherwise instead of commenting the password line in the `<database_params.conf>` file, just replace the string `appmanager` with the password of the your mysql.

startMySQL.bat (for windows)

rem mysqld-nt --defaults-file=%MYSQL_HOME%\my.ini -u root -b .. --standalone --port=13326

stopMySQL.bat (for windows)

rem mysqladmin -pappmanager -u root --port=13326 shutdown
startApplicationsManager.sh (for Linux)

if [\$? != 51]; then

. \$NMS_HOME/bin/stopMySQL.sh

fi

Starting the Failover Setup

- Make sure MySQL Server is started in node3 and check whether the *mysql.port* given in the *AMServer.properties* in Applications Manager match.
- First start Applications Manager in node1. This will get started and you can login to the console.
- Next start the Applications Manager in node2. This will not get started completely, unless the Applications Manager in node1 goes down. When node1 Applications Manager goes down, node 2 Applications Manager will get started along with polling, reporting etc.

Managed Server Failover Setup

The general setup of *Admin Server* will work in the above flow. With regards to Managed Server, you need to configure the multiple managed servers as against the single Admin Server.

Steps

- Need to start Primary Managed Server. This will register with Admin Server.
- Before starting the Secondary Managed Server, go to Admin Server and click Edit Managed Server (for which you are going to add failover support) and click failover details link. Here you need to give Secondary Managed Server details like (Host Name, Web Server port, SSL Port).
- Now you can start Secondary Managed Server.

Dual Database - Dual AppServer Architecture

For setting up failover support using replication, please refer this link.

Anomaly Detection

Anomaly detection helps you know if there is gradual performance degradation by defining Anomaly Profiles on performance metrics. By creating Anomaly profiles, you can define rules wherein the current data is compared with previously reported best data.

For eg., if the load on the server increases over a period of time, response time will gradually be affected. By using Anomaly detection, you would be able to detect this performance problem.

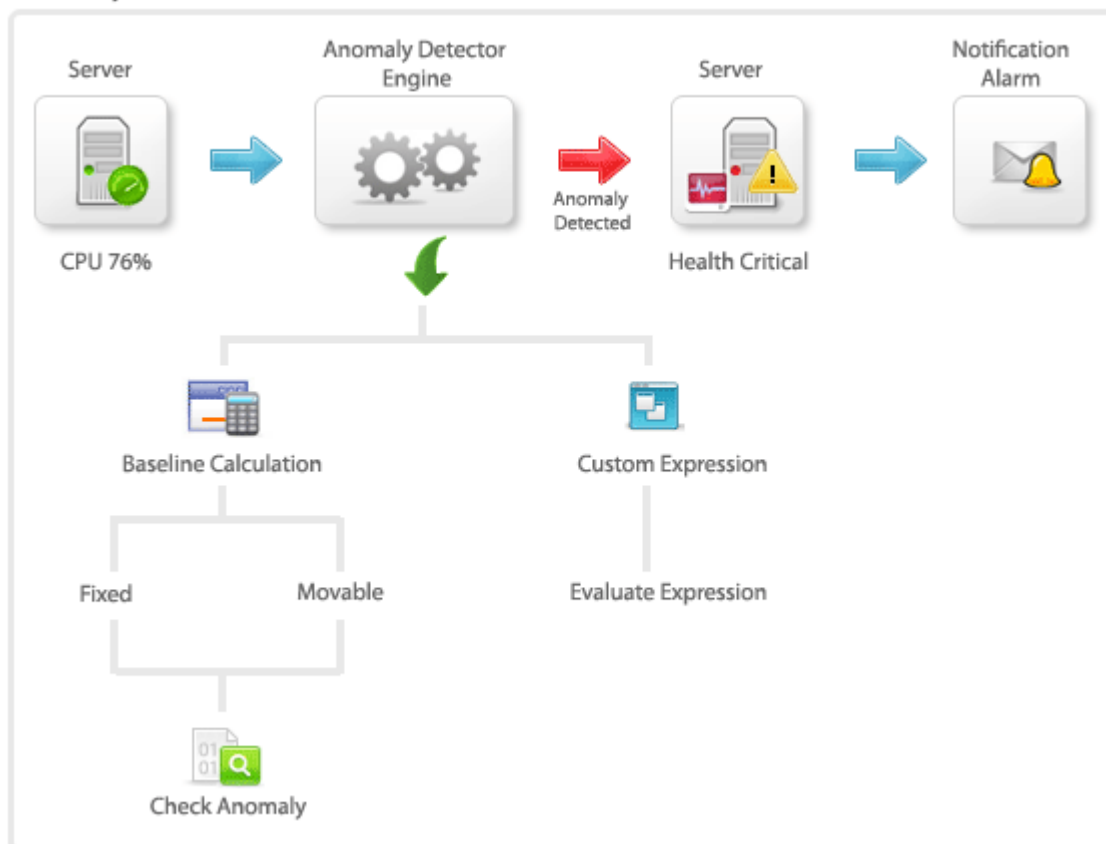
How does Anomaly Detection Work?

Anomaly profiles can be created based on:

- Baseline Values
- Custom Expressions

Anomaly Dashboard: This dashboard facilitates viewing through all the performance metrics and helps in easy troubleshooting.

Anomaly Detector Flow



Baseline Values:

Anomaly happens when the current set of values don't conform to the baseline range values. Current Attribute values are compared against the reported data in a particular week [baseline week].

- Define baseline - Baseline week can be calculated based on
 - Fixed Value: The week where the system has performed very well [there has been less number of alarms] will be chosen as reference/ baseline data range. After choosing the week for baseline comparison, then each day's value will be compared with the corresponding day of the baseline week. For eg. If you choose week 1 of August as baseline week, then every Monday's data will be compared with August week1's Monday values. Another usecase can be for festive time load. Anomaly profiles can be created for Christmas Holiday weekend and the performance metrics can be compared to know how effectively the system has performed.
 - Moving Value: Instead of fixing a baseline week, Previous week's reported data can be selected for comparison. Here, the baseline value will be changing according to the previous week's data.
- Specify the anomaly criteria - Set the upper limit and lower limit range to compare the current data with the baseline values.

Baseline data range will be formed based on the upper limit and lower limit values. These values can be used as % or as hard coded values. Eg, if the baseline value is 70 and if you had provided 10% as criteria for both upper and lower limits then the base line range will be between 64 to 77. Likewise if you had provided the criteria as 10 then the range will be between 60 to 80.

- Working - After comparing with the baseline data, if the current hour value does not come between the upper limit and lower limit configured, then alarms will be generated.
 - Lets set Aug 1st week of 2009 as the baseline data range.
 - Anomaly range is defined as 10% upper limit and 10% lower limit.
 - The deviation is calculated based on hourly values. So at 11 A.M, Tuesday of the Second Week, the Memory Utilization value will be compared with the values present at 11 AM, Tuesday of the 1st week. If the value deviates from the upper limit or lower limit, then an alarm will be generated.
 - After creating Anomaly profile, you have to associate the anomaly profile to the concerned attributes.

To create Anomaly Profile based on baseline values:

- Click on Anomaly Profile link. Click on New Profile
- In the Anomaly profile page, Give the Name for the new Anomaly profile you want to create.
- For baseline calculation, select the Baseline data range: You can choose between fixed baseline value [the appropriate week] or moving baseline value which is based on previous week's data.
- Define the allowed deviation from baseline. Alarms can be generated either based on percentage of upper limit, lower limit value or straightaway on hard coded comparison values. The generated Alarm will be cleared if the value falls in the baseline range [that is checked every hour]. Alarm can be critical or warning.
- Select the comparison method.
 - The recommended method would be to Compare last hour value directly with baseline value. Here, While comparing, hourly value will be taken into consideration and compared with the baseline value directly. For eg: Say if current time is 10:00 AM, Monday and if baseline date range is week 2. Then week 2, Monday 10:00 AM value will be taken for comparison and upper and lower limits will be applied as per the user configuration.
 - The other method would be to Compare values based on the corresponding difference with the previous hour. While comparing, the corresponding difference in hourly values would be taken into consideration.
For eg: If current time is 10:00 AM, we will take the difference between the values at 10:00 AM and 9:00 AM for comparison. A similar approach will be used for getting the baseline values.
- Finally click 'Create Anomaly profile'.

Custom Expressions

Anomaly is detected when current data doesn't conform to the user defined rules [based on system variables]. For eg., you can create a rule like Anomaly is to be detected when the current Last Hour Average Value is greater than twice the Six Hours Moving Average Value. Critical and Warning alarms can be set accordingly.

The system variables that can be used for forming custom expressions are

Expressions	Meaning
\$10D_MVA	Ten Days Moving Average
\$LastHourValue	Last Hour Average
\$6H_MVA	Six Hours Moving Average
\$30D_MVA	Thirty Days Moving Average
\$10H_MVA	Ten Hours Moving Average
\$7D_MVA	Seven Days Moving Average

To Create Anomaly Profile based on Custom Expressions:

- After choosing to create anomaly profile based on Custom Expressions, enter the profile name for the new anomaly profile.
- Critical Alarm : Create an expression like $\$LastHourValue > 10 * \$7D_MVA + (5 * \$30D_MVA)$. Then select the critical alarm from dropdown
- Warning Alarm : Create an expression like $\$LastHourValue \leq 25 * \$6H_MVA + (5 * \$10D_MVA)$. Then select the warning alarm from dropdown
- Save the Anomaly Profile.

To Associate Anomaly Profile:

- Go to the respective monitor details page. Choose the attributes for which you want to configure alarms. Click on Configure Alarms link.
- Threshold Details and Anomaly Details will be listed. Click on Anomaly Details tab.
- From the drop down box, Choose the appropriate attributes and associate them to the corresponding anomaly profiles.
- Save the alarm configuration

Note: A particular monitor's health will be made critical and EMail notification will be sent only if the user had associated EMail action to the health of the dependant attribute

Anomaly Dashboard

This dashboard facilitates viewing through all the performance metrics. It helps the user to intuitively scan through the hundreds of performance metrics with ease.

- If the health of any attribute / Monitor Group / Monitor has turned critical or if the availability is down, click on the icon for seeing the root cause analysis.
- Click on Use Anomaly Dashboard for troubleshooting to access the Anomaly Dashboard. You can access Anomaly Dashboard from Alarms tab too. In Alarms tab, all alarms whose health have turned critical are listed. Click on alarm message, it goes to Alarm Details page. In Alarm history table, you can find the Anomaly Dashboard icon
- In Anomaly Dashboard, You can choose to list only critical monitors or all monitors. Note: Critical state is based on the Anomaly profile associated to the attribute of the monitor.
- Base Metrics shows response time details and all other metrics by using current time but you can customize it using the change link. You can change the attribute and time. Note: The chosen time is used in all other calculation such as last hour value, 12 hour average etc.\
- Graphs: Last polled is last hour value. 12 hour is last 12 hour average values in graphical format [SparkSeries]. 7day segmented hour is shown as bar graph [Sparkline]. You can click through the columns to view the detailed reports.

- After associating anomaly profile to an attribute of a monitor, if the profile rule is violated, the monitor becomes critical and background of 12 hour graph will be red in color. By clicking on the column, you can see the detailed report like when anomaly value was reached, etc.

See Also

Associating Threshold and Action with Attributes

SLA Management Console For Managers

SLA Management 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 agreements (SLAs), the violation of which can be escalated by Email. By default, if the Manager is not explicitly associated to a Monitor Group, the Manager will be able to access all the Monitor Groups in the Manager Console. If the Manager is associated to a certain Monitor Groups, only those Monitor Groups will be shown in Manager Console - More

SLA Management 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 **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.

Events:

Upon clicking the Events tab, you can view the SLA details for all the Events associated. Events Volume statistics is shown as a bar graph. By default, the volume statistics for 'Today' is shown. A maximum of Events volume details of 12 business applications would be shown as bar graph. You have an option to view the Events volume statistics for other time periods like 'Yesterday', 'Last Week', 'Last month', etc.,

The Events Volume table, clearly lists down all the Business Applications associated with the different types of SLAs and it indicates whether events 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 Events

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 **Events**
- 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 Events Volume can be set as less than, equal to or less than equal to a particular number of Events 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.

Technical Support & 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 appmanager-support@manageengine.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\ManageEngine\AppManager10\bin>createSupportFile
```

After generating the support information file, e-mail it to appmanager-support@manageengine.com

If the support information file is large in size and our mail server blocks the same, then you can upload the file in our FTP site.

You will be provided details of the FTP service usage when you connect to our FTP server using "ftp ftp.zohocorp.com"

Server Name = ftp.zohocorp.com
user account = anonymous
password = "your email address"

Mail us 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 +1-925-924-9500 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 section 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
- **Installation Type:** Type can be Standalone, Managed Server or Admin Server
- **Load Factor:** The load factor follows the format 'x.y', where 'x' represents load on Applications Manager Server, while 'y' represents the load on the Database used by Applications Manager. A value of zero represents least loaded, while a value of nine represents most loaded.

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.
- **View Thread Dump Information:** Thread status in the JVM can be viewed here.
- **View Monitor Errors:** Error messages of monitors can be viewed here. You can see, if data collection has happened successfully or not at one go.

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.

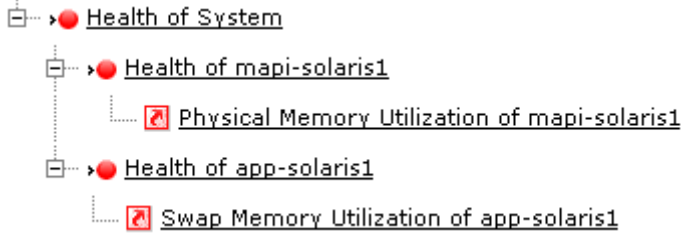
System Response Time

This graph provides information on the system's (where Applications Manager is installed) Response Time pattern for the last one hour.

Glossary

Terms	Definition
Action	<p>These are tasks to be performed to notify the user, when alarms are generated by Applications Manager.</p> <p>For example, while monitoring WebLogic server, if the user wants to be intimated when the server response time is greater than 1000ms, then an alarm is generated when the condition is met. The users are notified of the alarms through Actions such as sending e-mail, SMS, trap, and executing a command.</p>
Admin Activities	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.
Alarms	<p>Alarms are notifications generated based on Threshold / Health values .</p> <p>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 Alarms.</p>
Alarm Configuration	<p>This activity enables the user to associate a threshold profile with an attribute so that alarms are generated. It includes associating the action to be executed when an alarm is generated.</p> <p>Additionally, the dependencies for the "Health" attribute of a Monitor can also be configured.</p>
Attribute	Attributes are parameters/objects of a Monitor and they provide information about them. These are parameters whose values are set to threshold to generate alarms.
Availability	<p>An attribute that determines whether a system or application is available for use (Up or Down).</p> <p>For example, If a Web server is running, then the availability is up. 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.</p>
Monitor Groups	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.
Custom Monitor	<p>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).</p> <p>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.</p>
Dependencies	<p>Dependencies determine</p> <ul style="list-style-type: none"> • health of Monitor or Monitor Group • health or availability of Monitor Group

Terms	Definition
	<p>They consist of the dependent parameters of the Monitor based on which the severity of the health and availability is determined.</p> <p>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.</p>
Discover Network	Locating all Monitors running within a network range.
Enterprise OID in SNMP Trap	OID that uniquely distinguishes traps of different organizations, i.e. they vary for different vendors. This field applies only to SNMPv1 traps.
Generic Type in SNMP Trap	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.
Health	<p>An attribute that indicates the quality of Monitors, based on their dependencies.</p> <p>For example, 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 Availability as up >●.</p>
Monitoring	It is a continuous process that uses methodical collection and analysis of data to provide business management.
Monitor	<p>Application on which monitoring is performed. Monitor is an instance of a Monitor Type that is running in a port of a host.</p> <p>For example, 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.</p>
Monitor Type	<p>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.</p> <p>Different instances of these applications are Monitor.</p>
Mean Time to Repair (MTTR)	<p>The average time to repair a device or a system back to acceptable operating conditions. The term can also means, the time spent to restore a machine to operating condition after failure.</p> <p>This must be as low as possible. MTTR thresholds can be set to trigger root cause.</p>
Mean Time Between Failures (MTBF)	<p>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.</p> <p>This must be as high as possible. MTBF thresholds can be set to trigger root cause.</p>

Terms	Definition
Polling Interval	The time interval to monitor the different parameters configured for a Monitor.
RCA	<p>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.</p> <p>For example,</p>  <p>Expand the nodes to view the actual cause of the problem. Here, WebLogic Health is critical as Availability and Response Time (dependencies of Health) are also critical.</p>
Reports	They provide organized presentation of data that depicts the behavior of Monitor Types over a specified period of time.
Response Time	The time taken by a Monitor to react to a given input.
Severity	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.
SMTP Server	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.
SNMP OID	<i>Object identifier</i> (OID) that is used to uniquely identify each object variable of a MIB (Management Information Base).
Specific Type in SNMP Trap	When generic is set to Enterprise, a specific trap ID is identified.
SubNetMask	The subnet mask determines the maximum number of hosts on a subnetwork.
Threshold	<p>Threshold is the value that determines the severity of the alarm based on the pre-defined conditions.</p> <p>For example, 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.</p>
URL Monitors	Continuous URL monitoring service that monitors web pages. They verify the availability of specified, addressable, standard HTTP and HTTPS URLs of web pages.

Product FAQ

<http://apm.manageengine.com/Product-FAQ.html>

Web Client

Web Client Details

You can access Applications Manager Webclient via



- a. Programs Menu -> ManageEngine Applications Manager -> Applications Manager Start (Applications Manager starts and the webclient opens up)
- b. If you have already started Applications Manager, you can find a small icon on the Taskbar - Right click on the Applications Manager tray icon to access the webclient
- c. If Applications Manager is running in host - [Appln-Server] -port - 9090, you can directly access the webclient through the browser URL - <http://Appln-Server:9090>. You can view the monitors from an internet site or from any remote machine via this URL.

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.
- **Licensing:** 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.
- **Get Quote:** You can send a sales quote to Applications Manager Sales team based on your monitoring requirement..
- **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.




















Drag and Drop: The various tables in the webclient can be dragged and arranged as per your requirement.






- **Alarm Summary**  : Lists the recent critical alarms of Applications Manager. You can also click on the shades (representing the different severity) in the graph that will display the alarms 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 Alarms and Reports.












Note: By clicking on **Jump to** link, you can choose to log into ManageEngine ServiceDesk Plus / ManageEngine OpManager / ManageEngine OpStor from Applications Manager console itself. And also, in Enterprise Setup, you can choose to jump to the Managed Servers from Admin Server.

Icon Representation

The following are the icons used in Applications Manager and their significance:

Icon	Signifies
Severity	
	Health is Critical
	Health is Warning
	Health is Clear
	Health Unknown
	Availability Down
	Availability Up
	Health of Numerical Attribute is Critical
	Health of Numerical Attribute is Warning
	Health of Numerical Attribute is Clear
	Health of Numerical Attribute is Unkown
Monitor Type	
	JBoss Server
	Tomcat Server
	WebLogic Server , WebLogic Integration Server
	WebSphere Server
	Oracle Application Server
	SAP Server / SAP CCMS
	Microsoft .NET
	MS Office SharePoint Server
	IBM WebSphere MQ Series

Icon	Signifies
	Java Runtime
	J2EE Web Transactions
	Apache
	IIS Server
	PHP
	JMX Applications
	Active Directory
	Exchange Server
	Mail Server
	Web Services Monitoring
	Service Monitoring
	AdventNet JMX Agent
	SNMP
	Telnet
	Web Server
	MySQL Database Server
	Oracle Database Server
	MS SQL Database Server
	IBM DB2 Database Server
	Sybase Database Server
	Windows Performance Monitor
	File System Monitor
	Custom Monitor
	HTTP-URL Monitor and Sequence
	Linux Server

Icon	Signifies
	IBM AIX Server
	IBM AS400 / iSeries
	HP-Unix Server
	Solaris
	Windows Server
	FreeBSD Server
	Mac OS Server
	Unknown
	Script Monitor
	Database Query Monitor
	QEngine Script Monitor
	DNS Monitor
	LDAP Monitor
	Ping Monitor
	FTP/SFTP Monitor
	Novell Monitor
Report	
	Report generated by monitoring the attribute of the Monitor for 7 days.
	Report generated by monitoring the attribute of the Monitor for 30 days.
General	
	Edit icon to make changes in the configurations.
	Alarm Configuration icon where the thresholds and actions of the attributes are associated with the Monitor/ Monitor Group.
	Business View icon.

Custom Dashboards

By using Custom Dashboards feature, you can create Dashboards of your choice - like Status View of all the Databases, Status view of all Web Applications deployed in Tomcat Server. By adding the different widgets given, custom dashboards can be created.

This is in addition to the already created four Dashboards - Default Dashboard, Business View, Availability and QoS Worldwide (Quality Of Service Worldwide).

QoS Worldwide: This is done using 'embed webpage' widget . This dashboard helps you monitor your websites from outside your data center. Site24x7 is a website monitoring service that helps manage end user experience from a global point of presence. It helps monitor application and web service performance from a location closer to where your actual customers are.

Business Dashboards:

You can quickly configure your business metrics like customer wins, revenue, etc. It helps the Manager to align IT with business needs.

Monitor Group Template Dashboards:

After configuring a dashboard, you can save the settings as monitor group template. This monitor group template can then be applied for other monitor groups, thereby it becomes easier to create dashboards for monitor groups.

Create Dashboard

- Under home tab, click on **New Dashboard** link. It opens up the Create New Dashboard page.
- Enter the Dashboard **Name** and **Description**
- You can then configure the **layout** of the dashboard by selecting the number of columns and their size.
- You can save the dashboard settings as template and apply it to monitor groups. You have the option of applying the template to specific monitor groups or apply it across all the monitor groups.
- Then from the **Widget list**, you can choose the widgets you want to add.
- Click on **Create**. The new dashboard would be created with your choice of widgets.

- When you add a widget to the Dashboard, an empty widget will be added with an option to edit it. Click on edit widget icon and change the filter criteria for the widget until you get the desired data for the widget.

Widgets

Performance Widgets	<p>Top N Monitors: This widget displays Top N monitors based on a performance metric. To view the data, select a performance metric and select the monitors from which Top N should be listed. You have an option to view the graph for the selected time period.</p> <p>Performance Metric Widget: This widget displays the Snapshot value of a specific Monitor's performance metric. You have an option to view the graph for the selected time period.</p> <p>Threshold Breakers: This widget displays all the monitors which have exceeded the threshold for a performance metric. You have an option to view the graph for the selected performance metric.</p> <p>Tabular Data: This widget displays values in a tabular format, packs more data in a smaller area.</p>
Availability and Health Widgets	<p>Infrastructure Snapshot: This widget gives you a snapshot of availability and health of monitors grouped by Monitor Type.</p> <p>Availability & Health Status: Multiple Monitors: This widget lets you view the snapshot of monitors of specific Type.</p> <p>Last 24 Hours / 30 Days Availability History: This widget displays the Availability history for last 24 hours / 30 days for all monitors of selected Type.</p> <p>Last 24 Hours / 30 Days Health History: This widget displays the Health history for last 24 hours / 30 days for all monitors of selected Type.</p> <p>Availability, Health and Alarm Summary: This widget displays Availability and Health status and Alarm status for the selected Monitor category.</p>

Alarms	Last N Alarms: This widget displays the last N alarms for all the monitors.
Monitor Group Widgets	<p>Availability and Health Status: This widget displays all the Monitor Groups Availability and Health snapshot and Last 24 hours availability.</p> <p>Last 24 Hours / 30 Days Availability History: This widget displays the Availability history for last 24 hours / 30 days for all Monitor Groups.</p> <p>Last 24 Hours / 30 Days Health History: This widget displays the Health history for last 24 hours / 30 days for all Monitor Groups.</p> <p>Business View Widget: This widget displays the Business View of the Monitor Groups</p>
Utility Widgets	<p>Embed Web Page: This widget allows you to include a web page from another application into your dashboard. You can use this widget to integrate your custom dashboards.</p> <p>Bookmarks: This widget allows you to add weblinks to important documents, KBase articles.</p> <p>Custom HTML or Text: This widget allows you to add notes to your operator.</p>

Actions

Click on **Actions tab** to perform administrative operations for dashboards.

Add Widgets	Adds new Widgets
Edit Dashboard	Edits the custom created dashboards
Delete Dashboard	Deletes the selected dashboard
New Dashboard	Creates new dashboard

Publish Dashboard: The selected dashboard can be integrated with your Web Portal by using the Javascript Code Snippet given. So, those who can access your webportal can see the dashboard also.

Set as Default: The selected dashboard is set as the default dashboard. So, whenever you access the home tab, this dashboard would be displayed by default.

Note: By clicking on **Tabs Edit** icon you can choose the order in which the dashboard will be listed under the home tab


Custom Fields

As you monitor your applications and servers using Applications Manager, you may come across situations where certain important server-related data is not captured by the default fields present in Applications Manager. In such situations, you may want to add extra field types to capture that information. The 'Custom Fields' option allows you to configure these extra field types as per your business requirements.

Configuring Custom Fields

Click the *Custom Fields* button in the *Monitor Information* section of the monitor details page. This will open the *Custom Fields* section immediately below, where you can modify existing fields or add new fields.

There are 3 different tabs in the 'Custom Fields' section.

1. **Custom Fields:** In this tab, there are some preset fields such as Label, Impact, etc. You can edit the fields and specify their values as necessary. Apart from the default fields, you can add custom fields of your own if required. Just click the  icon in the right-hand corner of the 'Custom Fields' tab. This will open the 'Add/Remove Custom Fields' popup window where you can add new fields, edit current fields or remove unwanted fields.
2. **User/Owner:** This tab allows you to associate users to the particular monitor or monitor group. All types of user roles such as user, operator, administrator, and manager are supported.
3. **Location:** In this tab, you can specify information pertaining to the physical location of the server. The available fields include Location Name, Floor, building, city, state, country, postal code and zip code.

Note: The default values for custom fields of a monitor are inherited from the parent monitor group.

Custom Fields in Enterprise Edition

Although the custom fields option is available in both Professional and Enterprise editions of Applications Manager, there are a few minor differences in the way they can be configured in the Enterprise edition.

- From the admin server, you can add new fields, enable/disable fields, values, etc. for the monitors of the admin server. You will have full control over the monitors of the admin server.
- You cannot create or edit new fields in a managed server. You can only assign values to existing fields.

Note:

1. Custom fields cannot be configured for external device monitors (i.e. monitors from ManageEngine OpManager such as routers and switches). However, they can be assigned to a monitor group.
2. You can assign multiple values for certain fields such as label and user.

Mobile Web Client

ManageEngine Applications Manager mobile web client helps you perform comprehensive application monitoring on the go. Optimized for all types of smart phones available in the market, Applications Manager Mobile Client provides a convenient method to track critical applications, perform actions, receive alerts and identify issues quickly and easily from any location. The Mobile Web Client can be accessed using popular Mobile Web browsers.

The mobile client is adapted for efficiency on smartphones, and switching between customized views is just a few clicks away. There are Seven Monitor views in Mobile Client. The user can configure these views such that all relevant diagnostic and resolution information is available and easy to use.

- Infrastructure View
- Monitor Group View
- Dashboards
- Alarms
- Down Monitors
- Actions
- Search

Infrastructure View

Infrastructure view displays a list overview of all the monitors associated with a user classified into various categories, say Applications Servers, Database Servers etc. This view enlists the overall availability and health status and their health outages (the number of monitors in error by the total number of monitors). For usability reasons, the monitor types with critical health status are shown at top of the page. You can view the list of monitors of a particular type by clicking on any category under the list. By clicking on the monitor name will display a monitor details page where we can poll, manage/unmanage and ping the monitor.

Monitor Group View

Monitor group view lists all the configured top level monitor groups. This gives a clear view of the day's availability and health status of a monitor group or subgroup and the outages. This makes it easier to track if one of the monitors have failed. As in the Infrastructure View, you can click on a monitor group to see details like the total number of monitors associated to the group.

Dashboards

The dashboards view is for users who want a bird's eye view summarizing the dashboards alone. By clicking on any of the dashboards, you can list the widgets configured. Further, you can click on the widget names to know the widget details.

Alarms

By default, this view lists all the critical and warning alarms. You also have the option to list the clear alarms. The alarms are sorted based on the time of creation. By clicking on the health icons, you can get a summary of the alarm details. Clicking on an alarm opens the alarm details page where you can manage/unmanage alarm or clear the alarms. From an alarm details page you can also go the monitor or group details page by clicking on its name.

Down Monitors

This view lists all the 'down' or unavailable monitors associated to the user. From this view you also get a summary of the down monitor details like how long the monitor has been down. Clicking on the monitor name, displays a page where you can poll, manage/unmanage and ping the monitor.

Actions

This view will list all the action types associated with each of the monitors. Clicking on the action type lists the actions. You can view action details by clicking on the action name. From this view, you can execute the action. This is useful for executing actions like Windows service actions, Amazon EC2 actions and VM actions.

Search

You can display the Search page from the drop-down menu at the top of the page or from the tab at the bottom. You can use the search bar to search for any keyword. The Search result will have the list of monitors or monitor groups related to the keyword along with their availability and health status. You can go to the monitor/group details page by clicking on the monitor/group name.

The seven monitoring views in the Mobile Client of Applications Manager are tailored to meet the end user's needs and provides you with effective portable monitoring of your environment.

Appendix

- [Applications Manager Home](#)
 - [Data Collection - Host Resource](#)
 - [SNMP Agent Installation](#)
 - [SNMP Agent Configuration](#)
 - [Security/Firewall Requirements](#)
 - [Blog / Forum Articles](#)
 - [Add-On Pricing](#)
 - [Best Practices Guide](#)
-

Applications Manager Home

<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 <Program Files> directory of **C** drive in your system. In this case, <Applications Manager Home> denotes *C:\Program Files\ManageEngine\AppManager10*. In Linux, if Applications Manager is installed under home directory, then <Applications Manager Home> denotes *~/ManageEngine/AppManager1*

Data Collection - Host Resource

The important configuration details that are required while discovering host resource by Applications Manager are as follows:

Applications Manager Operating System	Monitor Operating System					
	Linux	Sun Solaris	HP-UX / Tru64	IBM AIX	FreeBSD	Windows
Linux	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Telnet mode of data collection. Default telnet port is 23. SSH mode of data collection. Default SSH port is 22 	<ul style="list-style-type: none"> Telnet mode of data collection. Default telnet port is 23. SSH mode of data collection. Default SSH port is 22 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> SNMP mode of data collection, default port is 161. HOST-RESOURCE-MIB must be implemented in the Agent.
Windows	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Telnet mode of data collection. Default telnet port is 23. SSH mode of data collection. Default SSH port is 22 	<ul style="list-style-type: none"> Telnet mode of data collection. Default telnet port is 23. SSH mode of data collection. Default SSH port is 22 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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:

<http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.1.1-1.rh9.i686.rpm?download>

Download the zip version of SNMP using the following URL:

<http://heanet.dl.sourceforge.net/sourceforge/net-snmp/ucd-snmp-4.2.6.tar.gz>

To **install using the rpm**, follow the steps given below:

1. Login as "root" user.
2. Before installing the new version of net-snmp, you need to remove the earlier versions of net-snmp in your machine. To list the versions of net-snmp installed in your machine, execute the following command:

```
rpm -qa | grep "net-snmp"
```

3. If there are already installed version in your machine, remove them using the command:

```
rpm -e <version of net-snmp listed as the output for previous command> --nodeps
```

4. If there are no previously installed versions in your machine, then execute the following command to install the new version:

```
rpm -i <new downloaded version of SNMP agent> --nodeps
```

To **install using the zip**, follow the steps given below:

Extract the file using following command:

```
tar -zxvf ucd-snmp-4.2.6.tar.gz
```


To install SNMP, follow the steps given below:

1. Login as *root* user.
2. Execute the command to set the path of the C compiler:
`export PATH=<gcc path>:$PATH`
3. Execute the following four commands from the directory where you have extracted the ucd-snmp:
 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. `net-snmp-5.1.1` package is available in the following url
`ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/net-snmp-5.1.1-sol8-sparc-local.gz`.
This package is for solaris8 on sparc.
6. `gunzip net-snmp-5.1.1-sol8-sparc-local.gz`.
7. `pkgadd -d net-snmp-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 `net-snmp` 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
`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

- Replace the lines

```
if [ -f /etc/snmp/conf/snmpdx.rsrc -a -x /usr/lib/snmp/snmpdx ]; then
    /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf -d 3 -f 0
fi
```

with

<Installation Directory>/sbin/snmpd

- Replace the line

/usr/bin/pkill -9 -x -u 0 '(snmpdx|snmpv2d|mibiiisa)'

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:

Monitors	Port Details
Windows	<p>WMI Mode of monitoring: Windows Management Instrumentation (WMI) -- Port: 445 Remote Procedure Call (RPC) -- Port: 135 WMI will use DCOM for remote communication and while communicating through DCOM, the target server (the server which is to be monitored by applications manager) by default will use any random port above 1024 to respond back. You have to connect to the target server and configure it to use a port with in the specified range of ports. You can follow the steps mentioned in this link : http://support.microsoft.com/kb/300083 for restricting the ports in the target server. Please note that you must specify at least 5 ports in this range for target server (you are normally recommended to open at least 100 ports - http://support.microsoft.com/kb/217351/EN-US/). This same range ports must be also opened in the firewall.</p> <p>SNMP Mode of monitoring: SNMP Agent Port: 161</p>
Linux / Solaris / AIX / HPUnix /Tru64 Unix	<p>Telnet Port: 23 (if mode of monitoring is Telnet) SSH Port: 22 (if mode of monitoring is SSH) SNMP Agent Port: 161 (if mode of monitoring is SNMP)</p>
JBoss	<p>Port in which JBoss is running (for eg., 8080) and also, the Hostname should be accessible. RMI Object port (eg., 4444)</p>
WebLogic	HTTP Port of WebLogic, for eg., 7001
Oracle Application Server	HTTP Port of Oracle Application Server, for eg., 7200

Monitors	Port Details
Tomcat	HTTP Port of Tomcat, for eg., 8080
WebSphere	HTTP Port of WebSphere (default:9080)
Oracle	HTTP Port of Oracle (default:1521)
DB2	HTTP Port of DB2 (default: 50000)
SQL Server	HTTP Port of SQL Server (default:1433)
MySQL	Port on which MySQL is running eg., 3306
Mail Server	SMTP Server port: 25 (default), to send mails from Applications Manager
Exchange Server	HTTP Port of Exchange Server (default:25)
Web Server - Apache / IIS / PHP	HTTP Port of Web Server (default:80)
JMX [MX4J / JDK 1.5]	<p>HTTP Port of JMX agent (default:1099)</p> <p>To monitor JMX behind firewall the following changes have to be done.</p> <p>Edit startApplicationsManager.bat/sh file. Add</p> <p>-Dmonitor.jmx.rmi.port=<port number for RMI socket communication> to the Java runtime options.</p> <p>Restart Application Manager server</p> <p>Ensure that you have the RMI Socket port (step1) and JNDI Port (step4) are opened up in the firewall</p> <p>Add the JMX Applications monitor after providing the relevant details.</p> <p>The monitor should be added successfully</p>
Service Monitoring	HTTP Port of Services (default:9090)
SNMP	HTTP Port of SNMP (default:161)
Telnet	HTTP Port of Telnet (default:23)
Web Transaction	Port in which the agent is deployed (default: 55555)
Hyper-V	Ports 135, 443 and 1025

When there is a two way communication, and the monitors need to access Applications Manager, then the following ports need to be opened.

Port	Description
WebServer Port: 9090	Should be opened for accessing the Applications Manager WebClient and also for monitoring WebLogic and JBoss.
Trap Port: 1620	If Traps are configured to be received in Applications Manager, then you need to open up Trap Port: 1620. More

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:

Monitors	Privileges
Windows	Administrator username/password [WMI mode]
Linux	Guest user privilege
Solaris	Guest user privilege
IBM AIX	Guest user privilege is sufficient but for collecting Memory related details, a user with "root" privilege is required. Hence, it is preferable to use a "root" account to view all details
HP Unix	Guest user privilege
MS SQL	System Administrator/Owner for the "master" database
MySQL	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.
DB2	Permission of "sysproc procedure" user of the DB2 database
Oracle	Permission of "system" user of the Oracle database
WebSphere	If Global Security is enabled, the username/password for the same. Else no username/password is required.

WebLogic	If WebLogic is authenticated, the username/password for the same. Else no username/password is required.
JBoss	If JBoss is authenticated, the username/password for the same. Else no username/password is required
Tomcat	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.
SNMP Agent	SNMP Community string with read privileges
Hyper-V	Administrator privileges to the root OS (Windows 2008 R2 and other supported Hyper-V versions)

Enterprise Edition

Path	Ports
Managed Server to Admin	SSL Port (default 8443)
Admin to Managed Server	SSL Port (default 8443) - for database syncing Webserver (default 9090)

Note: Production Environment gives you the configuration details that you need to take care of, when moving Applications Manager into Production.

User Management Security Policy

Applications Manager supports user management security policy for password validation.

Validation:

- Password should not be same/part of your Login name
- Password length should not be less than 8 characters
- Password length should not be greater than 255 characters
- Password should contain atleast 1 numeric character
- Password should contain atleast 1 special character
- Password should contain both uppercase and lowercase characters
- Password should not be the same as your last 4 passwords
- Password validation should be done in both server and client side.

Client side validation:

- Check for password length - should not be less than 8 characters
- Check for password length - should not be greater than 255 characters
- Check for password - should contain atleast 1 numeric character
- Check for password - should contain atleast 1 special character
- Check for password - should contain both uppercase and lowercase characters
- Check for password - should not be same/part of your Login name

Server side validation:

Above, the validation was given for client side. It is also done in server side. When Client validation has failed due to some malicious action (like truncating password) then server side validation should happen before changes happen to password.

- Check for password - should not be the same as your last 4 passwords
- Check for password - should contain atleast 1 numeric character
- Check for password - should contain atleast 1 special character
- Check for password - should contain both uppercase and lowercase character
- Check for password - should not be same/part of your Login name
- Password should not have more than three consecutive characters from the previous password

Account Lock-out Feature:

- User can try a maximum of 5 times with unsuccessful login, afterwards account automatically gets locked out.
- After 30 minutes of time, it gets locked out automatically.
- It will show the error message once it gets locked.

Single session per user:

- Application will allow the user to have only one session per user id at any point of time.
- Same user can not be connected to server from different machines/webclient at the same time.
- It will show the error message that “User Already logged in”

Forums / Blogs

Here are links to some interesting Forums and Blog posts:

Post	Description
Recognition in Gartner's Magic Quadrant	ManageEngine included in Gartner's Magic Quadrant for Application Performance Monitoring
Manage Virtual Machine Sprawl	Virtual Machine Sprawls: How can you keep them in check?
Manage Virtual Resources	Automate Virtual Machine Management with Applications Manager
Identify Problematic Java Code	Identify Java code consuming high CPU in Linux (linking JVM thread and Linux PID)
Multi-vendor Virtualization support	Now Monitor Hyper-V and VMware Servers from the Same Console
Server Troubleshooting	Reduce one step from your usual Server Troubleshooting Handbook
Flexible Alarm Management	Flexible Alarm Management for Performance Counters
Improve Operations Productivity	Improve Operations Productivity by Integrating Contextual Information using New Widgets for Custom Dashboards
Application Dependency Mapping	Application Dependency Mapping for better alarm management
Anomaly Detection	Proactively detect application performance problems with Anomaly Detection
Linux Startup	How to start Applications Manager when Linux boots (like starting Applications Manager as service in Windows) ?
Am I configuring properly?	Tips on easy configuration
Root Cause Analysis	Information on how best you can use Root Cause Analysis
Alarm Configuration made easy-1 Alarm Configuration made easy-2	Tips on easy alarm configuration

Post	Description
Custom Reports	Access Applications Manager Database and Generate Custom Reports / Dashboards
Migrating/Changing Applications Manager	How to migrate Applications Manager from machine to another?
HP-UX monitoring	Monitoring all the disk volumes in HP-UX machine
Script Monitor - Example1	How to monitor database tables of your choice using script monitor feature?
Script Monitoring - Example2	Script Monitoring - Monitor data from a particular row in the table
Script Monitor - Example3	How to monitor Sybase using scripts?
Builds	Advantages of Windows build over Linux build
SMS Alarms	Easy way to send SMS Alarms
Want a sound Alarm	Steps to configure sound Alarm from a remote machine
OpManager or Applications Manager	Helps you decide between OpManager and Applications Manager
Dell's OpManage	How to integrate Dell's OpManage with Applications Manager
GlassFish Application Server	How to monitor GlassFish Application Server
Response Time across Multiple Locations	Get to know how Enterprise Edition aids in comparing response time across multiple locations
Creating a proper threshold	Tips on easy Threshold Configuration
RCA Messages & Polls	Insight into RCA Messages
Create New Monitor Type	Create your own custom monitor types
Monitor Log Files and System Events	Log files and System Events monitoring
Intranet & Applications Manager	How to integrate AppManager in your Intranet

Add-Ons

Applications Manager offers 12 add-on features which are optional to use. These add-ons need to be purchased along with the base product.

Pricing Structure of Add-ons:

All the add-ons except Network Monitoring Connector and SAN Monitoring Connector are typically priced as a flat fee. You can monitor any number of resources as long as you are within the overall 'monitors' count.

For example, if you buy a 25 monitors license with SAP add-on, you can add any number of SAP monitors as long as the monitor count does not exceed 25.

Network Monitoring Connector and SAN Monitoring Connector Add-on Pricing:

The Network Monitoring Connector add-on connects ManageEngine Applications Manager to ManageEngine OpManager.

The SAN Monitoring Connector add-on connects ManageEngine Applications Manager to ManageEngine OpStor.

The price of these add-ons are not based on the monitor count. You need to buy these add-ons for integrating the respective product into Applications Manager.

For example, if you want to connect to ManageEngine OpManager, you need to install Applications Manager and OpManager with their respective licenses. The Network Monitoring Connector add-on just integrates OpManager into Applications Manager upon which the status of devices monitored in OpManager will be available in Applications Manager. Furthermore, the device details which are fetched from OpManager to Applications Manager are not counted as monitors in Applications Manager.

For more information about add-on pricing structure, please refer our online store.

Note: All the add-ons are included as part of the product. You can use them for free during your evaluation period. Once the evaluation period is over, you can use only those add-ons that you have purchased.

If you want to evaluate add-ons after your trial period has expired, you can request for a trial license by filling up this form in our website.

Troubleshooting

<http://apm.manageengine.com/index.html>

How to Demos

http://manageengine.com/products/applications_manager/howtodemos/index.html?help

Best Practices

http://www.manageengine.com/products/applications_manager/AM-BestPractices.pdf?help